Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm

Monika Gunjal[#1] , Jasmine Jha[*2]

[#]*M.E, CE Dept, L.J.Engg College, India*

[*]*M.E, I.T.Dept, L.J.EnggCollege,India*

Abstract **- Steganography is one of the methods of secret communication that hides the existence of message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. It is the process of embedding secret data in the cover image without significant changes to the cover image. A cryptography algorithm is used to convert the secret messages to an unreadable form before embedding. These algorithms keep the messages from stealing, destroying from unintended users on the internet and hence provide security. Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So the propose technique use a combination of steganography and cryptography for improving the security. The proposed technique use Discrete Cosine Transform (DCT) and Blowfish algorithm. The proposed method calculates LSB of each DC coefficient and replace with each bit of secret message. The proposed embedding method using DCT with LSB obtained better PSNR values. Blowfish algorithm is used for encryption and decryption of text message using a secret-key block cipher. This technique makes sure that the message has been encrypted before hiding it into a cover image. Blowfish is an improvement over DES, 3DES, etc designed to increase security and to improve performance.**

Keywords- **Steganography, Cryptography ,DCT, LSB, PSNR, MSE.**

I. INTRODUCTION

In the present era, communication through computer network requires more security. Two techniques are used for secret communication. One is cryptography, where the sender uses an encryption key to encrypt the message, this encrypted message is transmitted through the insecure public channel, and decryption algorithm is used to decrypt the message. The reconstruction of the original message is possible only if the receiver has the decryption key. The second method is steganography, where the secret message is inserted in another medium[9].

Steganography is the art of hiding information through original files in such a manner that the existence of the message is unknown. The term steganography is comes from Greek word steganos, which means, "Covered Writing". The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding process to restrict detection and/or recovery of the embedded data. While cryptography protects the content of messages, steganography hides the message so that intermediate persons cannot see the message[9].

A.Difference between Cryptography and Steganography

- The purpose of cryptography is to secure communications by changing the data into a form that can not be understood.
- Steganography techniques, on the other hand, hide the existence of the message itself, which makes it difficult for a third person to find out where the message is.
- Sometimes sending encrypted information may draw attention, while invisible information will not.
- Accordingly, cryptography is not the good solution for secure communication; it is only part of the solution. Both techniques can be used together to better protect information.

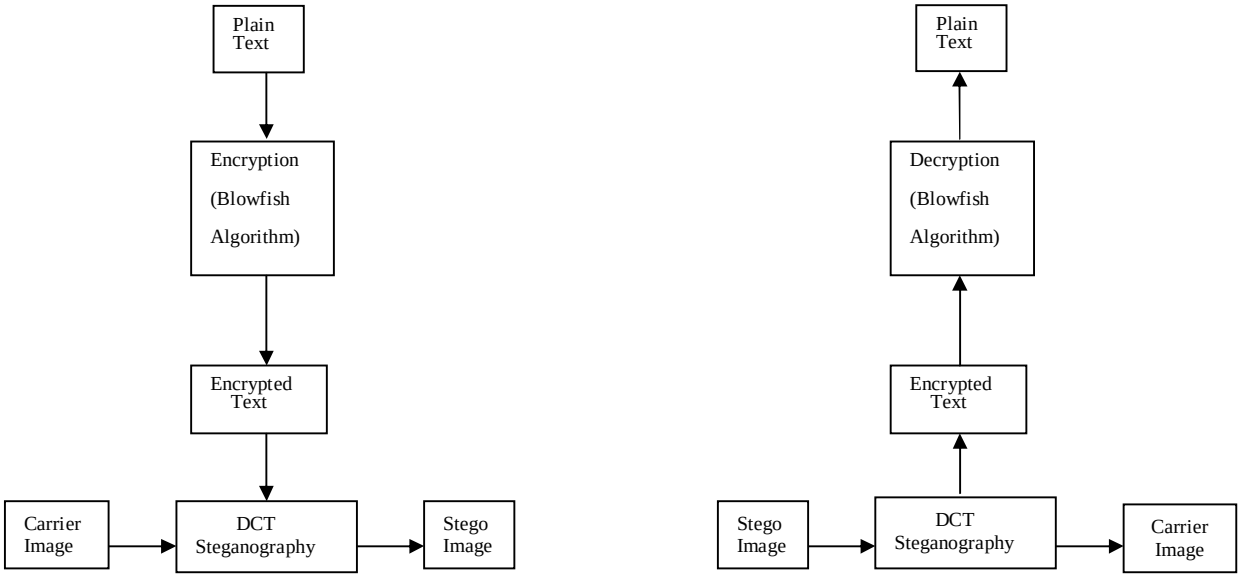
B. Motivation

- Industrial and military applications are driving the field
- Military applications – covert communications for:
  - CIA, FBI, other law enforcement
  - Battlefield scenarios
  - Steganalysis

- Industry: Record Industry Association of America (RIAA) looking for ways to protect copyrights of works that music producing companies own (Digital Millennium Copyright Act)
    - Illegal copying of songs onto CDs
    - Peer to peer networks allow distribution and easy access to lots of music

II. PROPOSED WORK

The Proposed method use combination of steganography and cryptography. The method use DCT steganography and Blowfish encryption algorithm. The encryption algorithm first encrypt the message and DCT steganography hide encrypted message into image. The Fig 1. display the flowchart of proposed method.



At Sender‘s side

At Reciever‘s side

Fig. 1 : Flowchart of Proposed Method

A. Algorithm of Proposed Method

Sender side:

Step-1: Write text message.(original message).

Step-2: Encrypt message using Blowfish algorithm.

Step-3: Select cover image.

Step-4: The cover image is broken into 8×8 block of pixels.

Step-5: Use DCT to transform each block Oi into DCT coefficient matrix Fi[a,b]=DCT(Oi[a,b]).

Step-6: Calculate LSB of each DC coefficient and replace with each bit of secret message.

Step-7: Write stego image.

Receiver side:

Step-1: Read the stego image.

Step-2: Divide the stego image into 8×8 block of pixels.

Step-3: DCT is applied to each block.

Step-4: Calculate LSB of each DC coefficient.

Step-5: Decrypt message using Blowfish algorithm.

Step-6: Get original message.

B. DCT Steganography[7]

DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It

transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. DCT is used in steganography as Image is broken into 8×8 blocks of pixels.

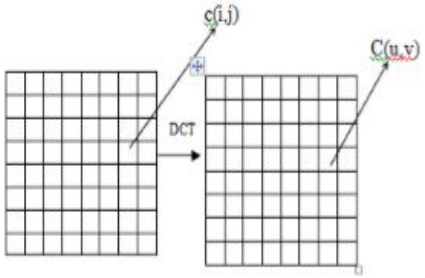


Fig .2 Discrete Cosine Transform of an Image[7]

$$C(u) = a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u = 0, 1, 2….. N-1

The general equation for a 2D (N by M image) DCT is defined by the following equation

$$C(u,v) = a(v)\sum_{i=0}^{N-1}\left[a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)\right] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

Wher e u, v = 0, 1, 2….N-1 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 column v of the DCT matrix.

C. Blowfish Encryption Algorithm[2]

Blowfish is a symmetric key block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

Blowfish has a variable-length key and 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of permutation depending on key, and a data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

Subkeys **:** Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.

The D-array consists of 18 32-bit subkeys:

D1, D2,..., D18.

There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255;

S2,0, S2,1,..., S2,255;

S3,0, S3,1,..., S3,255;

S4,0, S4,1,..., S4,255.

The sub keys are calculated using Blowfish algorithm

Step1: First initialize the P array and then the four S boxes in order with a fixed string.

Step2: XOR P1 with the first four 32 bits of key , XOR P2 with second 32 bits of key and so on for all bits of key (possibly up to P4). Repeatedly cycle through the key bits until the entire P array has been XOR ed with key bits.

Step3: Encrypt all the zero string with Blow fish algorithm using subkey described in step1 & 2.

Step4: Replace P1 and P2 with output of step 3.

Step5: Encrypt the output of step 3 using Blowfish with modified key.

Step6: Replace P3 and P4 with the output 5.

Step7: Continue the process of replacing all entries of P array and then all the four S boxes in order with the output of continuously changing Blowfish algorithm.

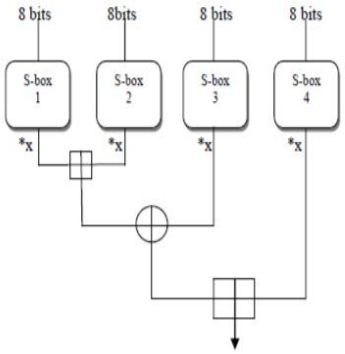


Fig. 3 Round Function of Fiestel Cipher [2] Encryption

The Round Function of Fiestel Cipher as shown in fig. (3).

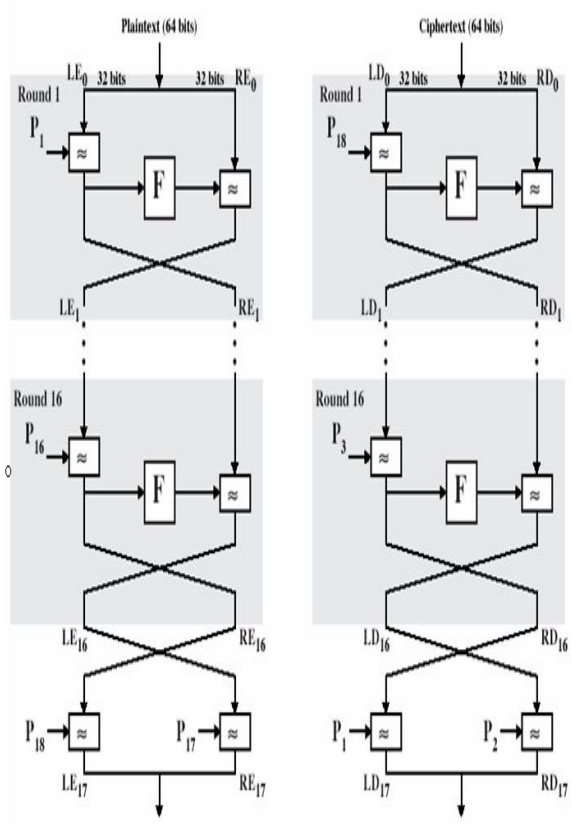
Encryption:

Blowfish is a Feistel network consisting of 16 rounds.

- The input is a 64-bit data element, x.
- Divide x into two 32-bit halves: xL, xR
- For i = 1 to 16:
- xL = xL XOR Pi
- xR = F(xL) XOR xR
- Swap xL and xR
- Next i
- Swap xL and xR (Undo the last swap.)
- xR = xR XOR P17
- xL = xL XOR P18
- Recombine xL and xR
- Function F
- Divide xL into four eight-bit quarters: a, b, c, and d
- F(xL) = ((S1,a + S2,b mod 2 32) XOR S3,c) + S4,d mod 2 32
- The resulting ciphertext is contained in the two variables LE17 and RE17

Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.

The Encryption and Decryption process of Blowfish algorithm as shown in fig.(4).



Cipher text plain text

(a) Encryption (b) Decryption

Fig.4 Blowfish Encryption and Decryption

III. EXPERIMENTAL RESULTS

The results are taken in matlab programming. The PSNR and MSE values are calculated using equation (1) and (2) .The PSNR and MSE values are displayed in Table I.

The Peak Signal-to-Noise Ratio (PSNR) is defined as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad \textbf{(1)}$$

The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is

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

Where M and N are the number of rows and columns in the input images, respectively.

The experimental results of proposed method as shown in table I.

Data Bytes	Image Size	PSNR in DB	MSE
656	600*450(im1)	72.7508846	0.004122
	800*600(im2)	71.7508846	0.004379
800	600*450(im1)	72.3669633	0.003800
	800*600(im2)	71.0083669	0.004127
1104	600*450(im1)	69.7184170	0.006993
	800*600(im2)	70.2059991	0.006250

Table I. The experimental results of proposed method

The Peak Signal-to-Noise Ratio (PSNR) is calculated to measure the quality of stego image. The PSNR is calculated in db. Larger PSNR indicates better quality of an image.

For 800*600 pixels image**,** The fig.(5) shows that PSNR of images becomes high when the size of embedded data is less.

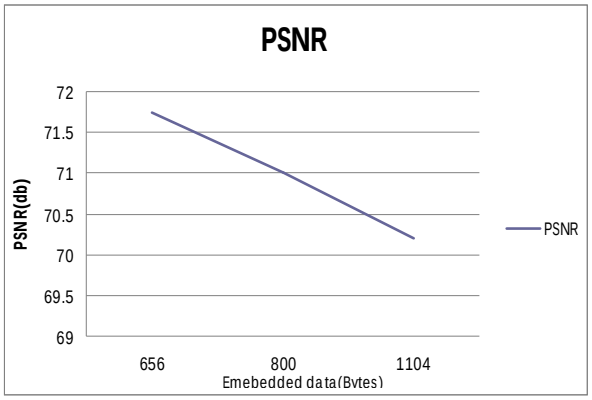


Fig. 5 PSNR Vs. DATA

(For 800*600 pixels image)

For 600*450 pixels image, The fig. (6) shows that PSNR of images becomes high when the size of embedded data is less.

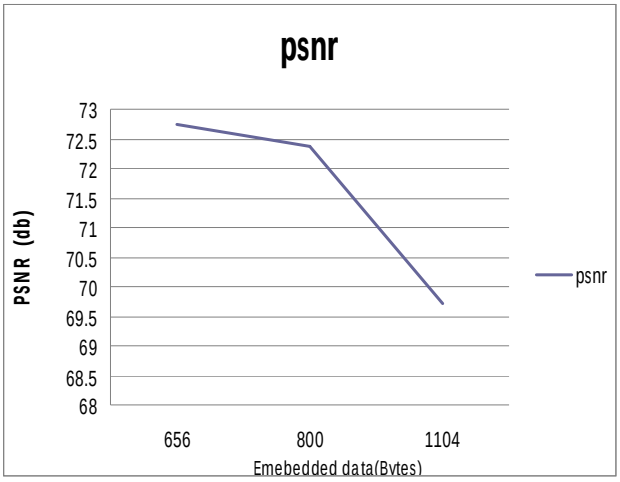


Fig. 6 PSNR Vs. DATA

(For 600*450 pixels image)

The fig 7 is cover image and fig 8 is the stego image and PSNR value of this image is 72.7508846.The size of the cover image is 600*450 pixels.

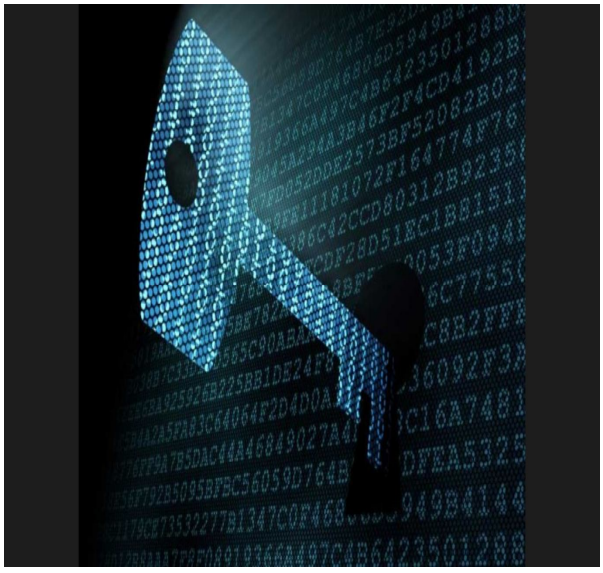


Fig. 7 Cover Image (im1)

Fig. 8 Stego image

The histogram of the cover image and stego image, as shown in fig.9 and fig.10 respectively.

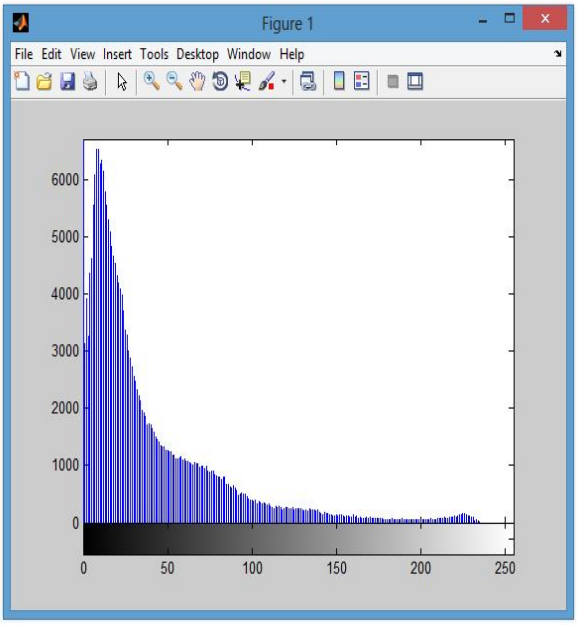


Fig. 9 Histogram of cover Image(im1)

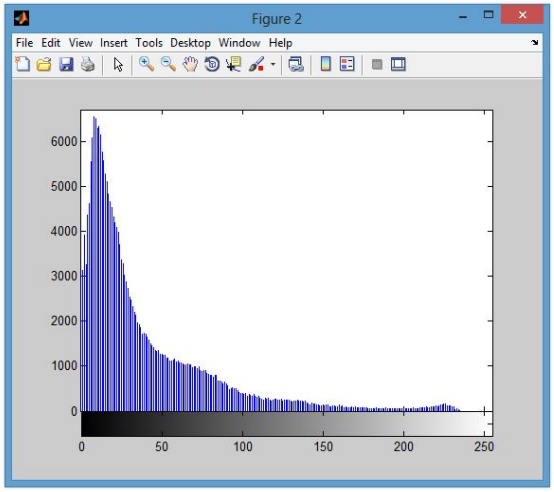


Fig.10 Histogram of Stego Image

The results of PSNR values obtained from the DCT,DWT and Proposed method(DCT with LSB) is displayed in Table II. The PSNR value is increased using proposed method.

	PSNR(db)
Using DCT	48.131
Using DWT	50.134
Using Proposed Method(DCT with LSB)	71.251

Table II. Comparison Results

IV. CONCLUSION

The proposed method use combination of DCT with LSB and Blowfish Algorithm. To provide high security steganography and cryptography are combined together. This system encrypts secret information before embedding it in the image. Steganography use Blowfish algorithm for encryption and decryption. From comparative study of some cryptography Techniques, blowfish has better performance than other algorithms. The integrated approach of combining DCT with LSB and Blowfish provide secure transfer of payload. The proposed method provide better quality of an image means that provide high PSNR value.

REFERENCES

[1]. Mrs.Archana S. Vaidya, Pooja N. More., Rita K. Fegade., Madhuri A.Bhavsar., Pooja V. Raut, "Image Steganography using DWT and Blowfish Algorithm" Volume 8, Issue 6 (Jan. - Feb. 2013).

[2]. Ajit Singh, Swati Malik , "Securing Data by Using Cryptography with Steganography", Volume 3, Issue 5, May 2013.

[3]. Shahana T, "An Enhanced Security Technique for Steganography Using DCT and RSA", Volume 3, Issue 7, July 2013.

[4]. Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for data hiding using CryptographyAnd Steganography ".

[5]. M. Anand Kumar and Dr.S.Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms", I. J. Computer Network and Information Security, 2012.

[6]. Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud , "Evaluating The Performance of Symmetric Encryption Algorithms",Vol.10,No.3, May 2010.

[7]. Stuti Goel, Arun Rana & Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography", Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 Year 2013 .

[8]. Dr. Ekta Walia , Payal Jain , Navdeep, "An Analysis of LSB & DCT based Steganography",Vol. 10 Issue 1 (Ver 1.0), April 2010.

[9]. Pratap Chandra Mandal, "Modern Steganographic technique: A survey",International Journal of Computer Science & Engineering Technology(IJCSET), Vol. 3 No. 9 Sep 2012.

[10]. E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", Volume 2, Issue 7, July 2012 .

[11]. Rajinder Kaur, Er. Kanwalpreet Singh , "Comparative Analysis and Implementation of Image Encryption Algorithms" International Journal of Computer Science and Mobile Computing Vol.2 Issue. 4, April- 2013.

[12]. C.Gayathri , V.Kalpana , "Study on Image Steganography Techniques " International Journal of Engineering and Technology (IJET) Vol 5 No 2 Apr-May 2013.

[13]. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", 987-161284-908-9/11 © 2011 IEEE.

[14]. Yam bern Jina Chanu, ThemrichonTuithung, Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", 978-1-4577-0748-3/12 © 2012 IEEE

[15]. AL.Jeeva,Dr.V.Palanisamy,K.Kanagaram,"Comparative analysis of performance efficiency and security measures of some encryption algorithms", Vol. 2, Issue 3, May-Jun 2012.