A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryptography

M. Indrasena Reddy
Asst. Professor
RGMCET
Nandyal

V. UdayKumar
Asst. Professor
RGMCET
Nandyal

K. Subba Reddy
Assoc. Professor
RGMCET
Nandyal

ABSTRACT
Steganography and cryptography methods are used together with wavelets to increase the security of the data while transmitting through networks. In the discrete wavelet transform, an image signal can be analyzed by passing it through an analysis filter bank. This analysis filter bank consists of a low pass and a high pass filter at each decomposition stage. Another technology, the digital watermarking is the process of embedding information into a digital (image) signal which may be used to verify its authenticity or the identity of its owners. The watermark to be embedded is 'text'. Before embedding the plain text into the image, the plain text is encrypted by using Data Encryption Standard (DES) algorithm. The plain text can be any sentence in English, and the key can be anything in English with a length of 8-characters. The encrypted text is embedded into the LL subband of the wavelet decomposed image using Least Significant Bit (LSB) method. Then the inverse wavelet transform is applied and the resultant image is transmitted to the receiver. At the receiver's end, the image is transformed using wavelet, from the LL subband the encrypted text is extracted by using the LSB method and the result is decrypted using DES.

Keywords
Steganography, Cryptography Wavelet, Digital Watermarking.

1. INTRODUCTION
Cryptography means 'Secret Writing'. However we use the word to refer to the science and art of transforming messages to make them secure and immune to attacks. Cryptographic algorithms are of two types [1]. In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared. In Asymmetric-key cryptography, the sender uses the public key and the encryption algorithm to encrypt the data,where as the receiver uses the private key and the corresponding decryption algorithm to decrypt the data.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message[2]. Hiding information into a media requires following elements.

- The cover media(*C*) that will hold the hidden data
- The secret message (*M*), may be plain text, cipher text or any type of data
- The stego function (*Fe)* and its inverse (*Fe-1*)
- An optional stego-key (*K*) or password may be used to hide and unhide the message[3].

The common modern technique of steganography exploits the property of the media itself to convey a message. The following medias are the candidate for digitally embedding message:

- Plaintext
- Still imagery
- Audio and Video
- IP datagram.

Combining encryption with steganography allows for a better private communication. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On the other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It relies on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that could be exploited. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable [4, 5, 6].

Steganography includes the hiding of media like text, image, audio, video files, etc. in other media of the same type or of different type. Later, the message hidden in the selected media is transmitted to the recipient. At the receiver end, the reverse process is implemented to recover the original message [7].

Many ideas and techniques have been proposed to secure data i.e., mainly concealing of text in images. The simplest method to do the same is Least Significant Bit replacement method in steganography. But it has its own limitations [8].

A '*wavelet*' is a kind of mathematical function used to divide a given function or continuous-time signal into different frequency components and study each component with a resolution that matches its scale. The wavelet transform is a multi-resolution technique, which can be implemented as a pyramid or tree structure and is similar to sub-band decomposition[9,10,11].There are various wavelet transforms like Haar, Daubechies, Coiflet, Symlet and etc. They differ with each other in the formation and reconstruction.

The wavelet transform divides the original image into four subbands and they are denoted by LL (low-low), LH (low-high), HL (high-low) and HH (high-high) frequency subbands. The HH subimage represents diagonal details (high frequencies in both directions – the corners), HL gives horizontal high frequencies (vertical edges), LH gives vertical high frequencies (horizontal edges), and the image LL corresponds to the lowest frequencies which is shown in Fig 2.. At the subsequent scale of analysis, the image LL undergoes the decomposition using the same filters, having always the lowest frequency component located in the upper left corner of the image. Each stage of the analysis produces next 4 subimages whose size is reduced twice when compared to the previous scale. I.e. for level 'n' we get a total of '4+ (n-1) *3' subbands. The size of the wavelet representation is the same as the size of the original. The Haar wavelet is the first known wavelet and was proposed in 1909 by Alfred Haar. Haar used these functions to give an example of a counting orthonormal system for the space of square-integrable functions on the real line. The Haar wavelet scaling function coefficients are h {k} = {0.5, 0.5} and wavelet function

coefficients are g {k} = {0.5, -0.5} [12]. This new proposed method overcomes this draw back [12, 13,14,15].

2. PROPOSED ENHANCEMENT

In this paper, a new method is used to send the data in a more secured manner. The given text which is to be transmitted is encrypted with one of the symmetric key techniques: DES with the given key. In this process by using the key, the given text is encrypted. Then this resultant text is decrypted with the same key. (Here, the key is of length 56-bit.) Then, that cipher text is embedded into the LL subband of the wavelet transformed image. The method to embed the data is the Least Significant Method. This method is described in Algorithm-1. Note that, as we are modifying the LSB (±1 or no change to the given pixel value) our human eye cannot find the difference between the original image and the watermarked image. Once the cipher text is embedded into the LL subband, inverse wavelet transform is applied. Then this resultant image is sent to the receiver. In the available literature they used independently cryptography, steganography and wavelets. In this paper to increase the security for the image the authors are used cominely cryptography, steganography and wavelets. Existing and proposed methods are presented in Table 1.

Table 1: Existing and proposed methods

	Crypto-graphy	Stegano-graphy	Wavelets	present
Encryption & Decryption	√	×	×	√
Hiding the data into the image	×	√	×	√
Wavelet transformation	×	×	√	√
Inverse Wavelet transformation	×	×	√	√

3. IMPLEMENTAION

DES (the Data Encryption Standard) is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1. The algorithm is best suited to implementation in hardware, probably to discourage implementations in software, which tend to be slow by comparison. However, modern computers are so fast that satisfactory software implementations are readily available.

DES is the most widely used symmetric algorithms in the world, despite claims that the key length is too short. Ever since DES was first announced, controversy has raged about whether 56 bits is long enough to guarantee security. The key length argument goes like this. Assuming that the only feasible attack on DES is to try each key in turn until the right one is found, then 1,000,000 machines each capable of testing 1,000,000 keys per second would find (on average) one key every 12 hours. Most reasonable people might find this rather comforting and a good measure of the strength of the algorithm.

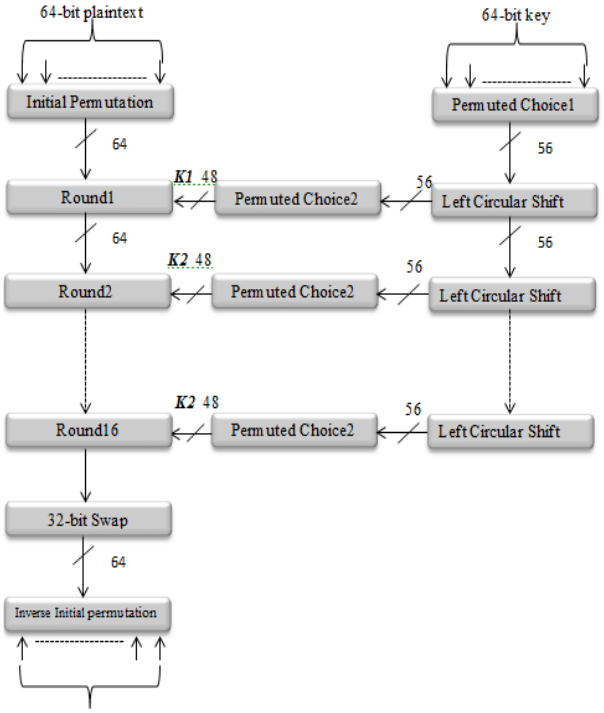

Fig: 1. General Description of DES Encryption Algorithm

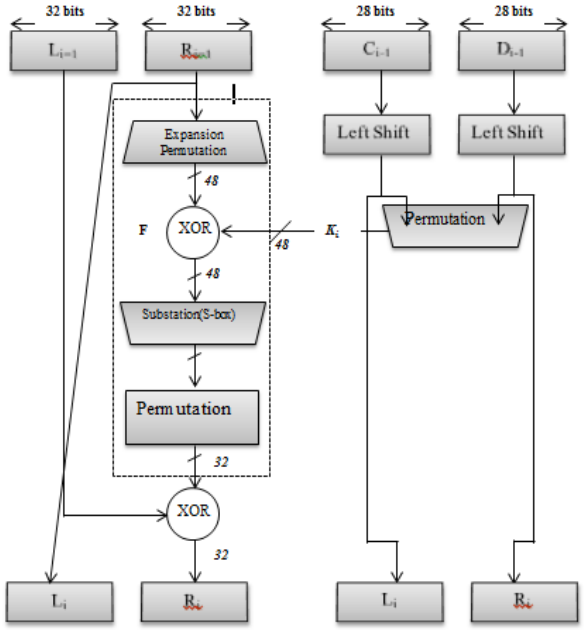

Fig: 2. Single rounds in DESNormal or Body

3.1 Conversion from Plain text to Ciphertext

DES is a **block cipher**--meaning it operates on plaintext blocks of a given size (64-bits) and returns ciphertext blocks of the same size. Thus DES results in a **permutation** among the 2^64 (read this as: "2 to the 64th power") possible arrangements of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block **L** and a right half **R**. (This division is only used in certain operations.)

Example: Let **M** be the plain text message **M** = 0123456789ABCDEF, where **M** is in hexadecimal (base 16)

format. Rewriting **M** in binary format, we get the 64-bit block of text:
M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110
1111
L = 0000 0001 0010 0011 0100 0101 0110 0111
R = 1000 1001 1010 1011 1100 1101 1110 1111
The first bit of **M** is "0". The last bit is "1". We read from left to right.
DES operates on the 64-bit blocks using key sizes of 56- bits. The keys are actually stored as being 64 bits long, but every 8th bit in the key is not used (i.e. Bits numbered 8, 16, 24, 32, 40, 48, 56, and 64). However, we will nevertheless number the bits from 1 to 64, going left to right, in the following calculations. But, as you will see, the eight bits just mentioned get eliminated when we create subkeys.
This is the encrypted form of **M** = 0123456789ABCDEF: namely, **C** = 85E813540F0AB405.
Decryption is simply the inverse of encryption, following the same steps as above, but reversing the order in which the sub keys are applied.

3.2 Wavelet Based Digital Watermarking with DES Encrypted Text

A 'wavelet' is a kind of mathematical function used to divide a given function or continuous-time signal into different frequency components and study each component with a resolution that matches its scale. The wavelet transform is a multi-resolution technique, which can be implemented as a pyramid or tree structure and is similar to sub-band decomposition.
There are various wavelet transforms like Haar, Daubechies, Coiflet, Symlet and etc. They differ with each other in the formation and reconstruction. The wavelet transform divides the original image into four subbands and they are denoted by LL (low-low), LH (low-high), HL (high-low) and HH (high-high) frequency subbands. The HH subimage represents diagonal details (high frequencies in both directions – the corners), HL gives horizontal high frequencies (vertical edges), LH gives vertical high frequencies (horizontal edges), and the image LL corresponds to the lowest frequencies which is shown in Fig:3

Fig:3 (a). Original Image (b) Level-1 Wavelet Transformed Image.

At the subsequent scale of analysis, the image LL undergoes the decomposition using the same filters, having always the lowest frequency component located in the upper left corner of the image. Each stage of the analysis produces next 4 subimages whose size is reduced twice when compared to the previous scale. I.e. for level 'n' we get a total of '4+ (n-1) *3' subbands. The size of the wavelet representation is the same as the size of the original.

The Haar wavelet is the first known wavelet and was proposed in 1909 by Alfred Haar. Haar used these functions to give an example of a counting orthonormal system for the space of square-integrable functions on the real line. The Haar wavelet scaling function coefficients are h {k} = {0.5, 0.5} and wavelet function coefficients are g {k} = {0.5, -0.5}. The Daubechies wavelets [10] are a family of orthogonal wavelets defining a discrete wavelet transform and characterized by a maximal number of vanishing moments for some given support. With each wavelet type of this class, there is a scaling function which generates an orthogonal multiresolution analysis.

3.3 Methodology

In this process by using the key, the given text is encrypted. Then this resultant text is decrypted with the same key. (Here, the key is of length 56-bit.) Then, that cipher text is embedded into the LL subband of the wavelet transformed image. The method to embed the data is the Least Significant Method. This method is described in Algorithm-1. Note that, as we are modifying the LSB (±1 or no change to the given pixel value) our human eye cannot find the difference between the original image and the watermarked image. Once the cipher text is embedded into the LL subband, inverse wavelet transform is applied. Then this resultant image is sent to the receiver.
Algorithm-1: Least Significant Method

Begin

Step-1: Read the value of the pixel.
Step-2: Convert it to its equivalent binary form.
Step-3: Modify the least significant bit accordingly.

End

At the receiver's end, the receiver does the forward wavelet transform of the received image. Now, from the LL subband, the text is extracted. The extracted text which is encrypted form is decrypted using the one key.
The encryption and decryption process using these one key is shown in Fig: 4. The entire process of the method is shown in the form a flow chart in Fig: 4

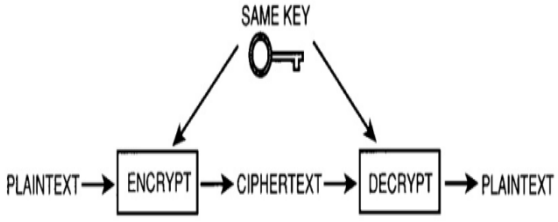

Fig: 4 Data Encryption and Decryption in DES

The Fig: 5. Shows about the process of encrypting the data into the image by using wavelet transform at the sender side and decrypting the data at receiver side of an image by using inverse wavelet transform.
The flow chart of the proposed method is shown in the Fig. 5.

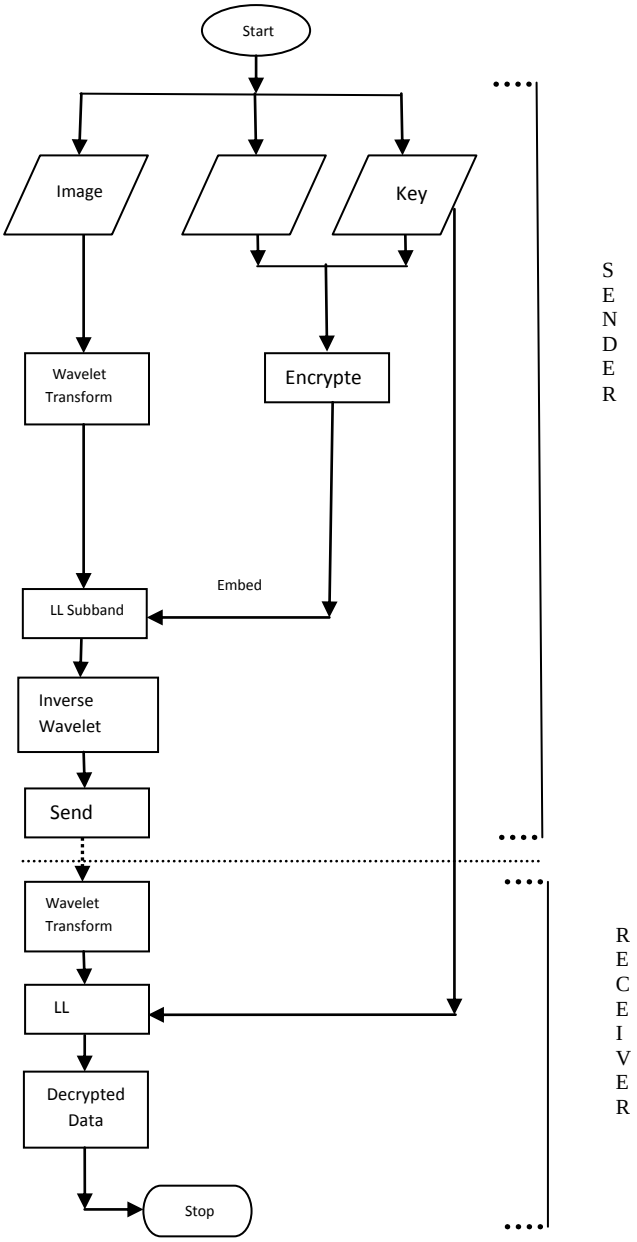

Fig. 5.The flow chart of the proposed method.

.

4. SOURCE CODE

From Sender Side:

```
Clear all;
Cls;
x1=imread('E:\lena.jpg');
x1=rgb2gray (x1);
ciphertext=dec1keyencrfunc ();
%Actually there is no use of LL. Simple I am sending it
 %Now we have to embed the Hexaciphertext into the image first 8 lines
%First two hexes into first line
%Second pair (3rd and 4th ) of hexa into second line of LL ...
binarycipher=binaryconverter1 (ciphertext);
waveres=sumdiff (x1); %Calling the wavelet transform function
[Resow, rascal] =size (weavers);
  LL (1: (resow/2), 1: (resow/2)) =fix ( weavers (1: (resow/2), 1: (rescol/2)) ); %Rounding the values using fix
  HL (1: (resow/2), 1: (rescol/2)) =waveres (1: (resow/2), (rescol/2)+1: rascal);
  LH (1: (resow/2), 1: (rescol/2)) =waveres ((resow/2)+1: resrow, 1: (rescol/2));
  HH (1: (resow/2), 1: (rescol/2)) =waveres ((resow/2)+1: resrow, (rescol/2)+1: rascal);
embedres=embeddingfunc (LL, binarycipher); %Here  I am sending send LL also
[Cipherrowsciphercols] =size (binarycipher); %Keeping the result in LL original
LL (1: cipherrows, 1:8) =embedres;
res11= [LL HL;
     LH HH];
res11=fix (res11);
res2=haarinv (res11);
%imview (res2, []);
Subplot (1,3,1), subimage (x1), title ('ORIGINAL IMAGE');
Subplot (1,3,2), subimage (mat2gray (wavers)), title ('WAVELET IMAGE');
Subplot (1,3,3), subimage (mat2gray (res2)), , title ('WATERMARKED IMAGE');
fid = fopen('D:\kk115.txt','w+');       fwrite(fid,res2);
```

From Receiver Side

```
Clear all;
Cls;
fid=fopen('D:\kk115.txt','r+'); %Read the received text file and convert into an image
A = fread (FID);
t=1;
For i=1: 256
   For j=1: 256
        X (j, I) =a (t);
        t=t+1;
   End
End
 res22=x;
waveres=sumdiff (res22); %Calling the wavelet transform function
[Resow, rascal] =size (weavers);
 LL (1: (resow/2), 1: (resow/2)) =fix ( weavers (1: (resow/2), 1: (rescol/2)) ); %Roundin the values using fix
   HL (1: (resow/2), 1: (rescol/2)) =waveres (1: (resow/2), (rescol/2)+1: rascal);
   LH (1: (resow/2), 1: (rescol/2)) =waveres ((resow/2)+1: resrow, 1: (rescol/2));
   HH (1: (resow/2), 1: (rescol/2)) =waveres ((resow/2)+1: resrow, (rescol/2)+1: rascal);
 Subplot (1,2,1), subimage (mat2gray (res22)), title ('RECEIVED IMAGE');
Subplot (1,2,2), subimage (mat2gray (wavers)), title ('WAVELET IMAGE');
 extra1=extractionfun2 (LL, 16); %By this we get the result in hex in decrypted form
   %Now decrypt the received data
decrres=des1keydecrfunc (extra1)
```

5. RESULTS AND DISCUSSION

By taking an example the text '**udayuday**' is taken as input. For this text, the corresponding hexa representation is '**7564617975646179'**. Key- '**asdfghjk'** which is of length 8 characters are taken to alter the message 'Gandhiji'. The result after the encryption using Key is '**E2DDF6ABE534CFF2**'. Now this result is decrypted using Key which results '**7564617975646179**'. Now this data is the one which is going

to be embedded into the image. At the other end, the given image is transformed using Haar forward wavelet transform to get the LL, LH, HL and HH subbands. The data which are the result of the above method is embedded into the LL subband. After that, the image is transformed back to the original form using Haar inverse wavelet transform.

After receiving the image from the sender, the image is once again transformed using Haar forward wavelet to extract the hidden data and that data is decrypted using the steps given in Fig.6 Finally, the original message is received as 'Gandhiji'. The following screen shots for this entire process are shown in Fig:6.1(a) to Fig:6.1(f).

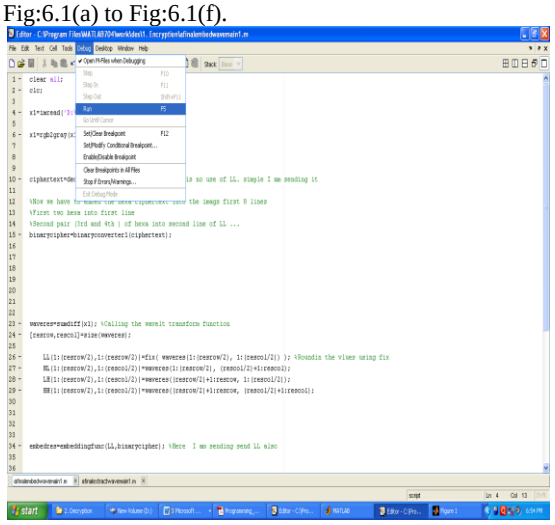

Fig 6.1(a) shows the execution of sender program

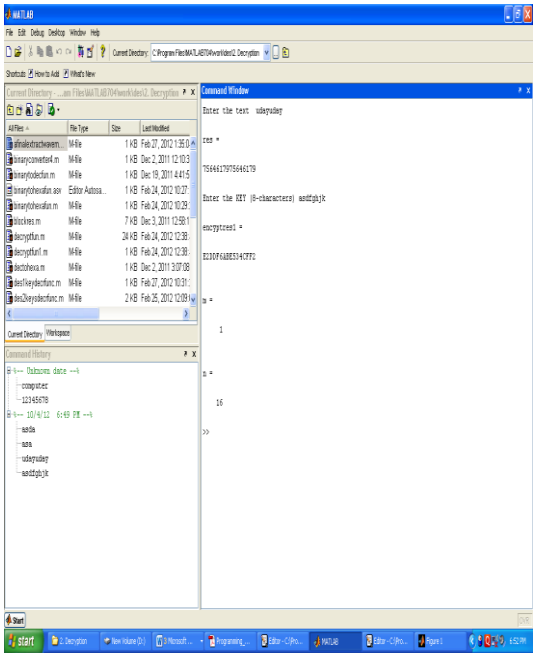

Fig 6.1(b) we enter the text and key

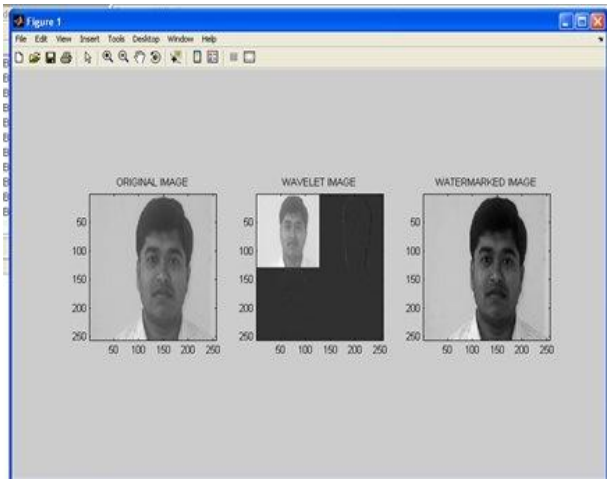

Fig 6.1(c) shows the setgo image i.e., both Wavelet image and Watermarked image

Fig: 6.1(a),(b) and (c).The results at sender side

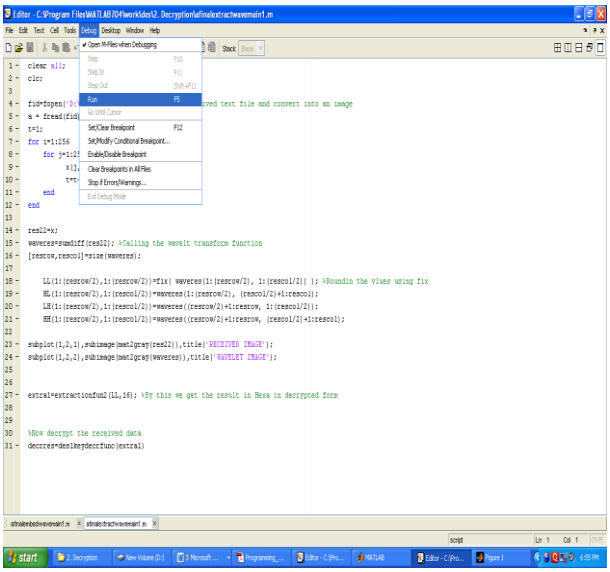

Fig 6.1(d) shows the receiver side execution

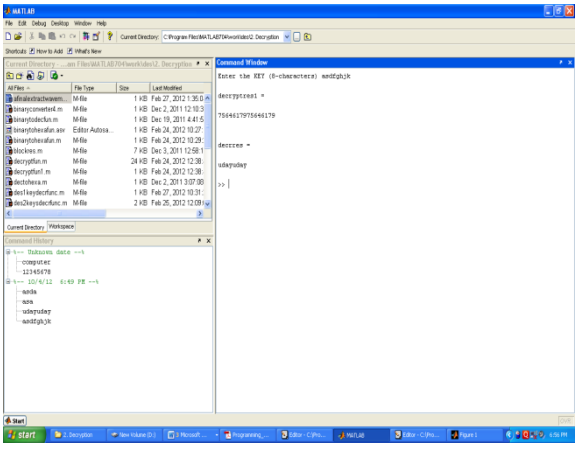

Fig 6.1(e) shows the extraction of text using decryption

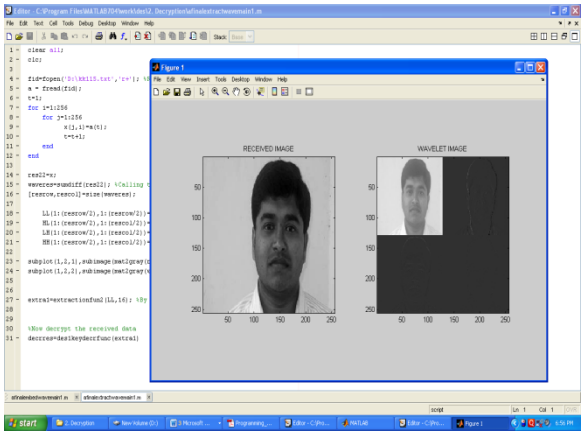

Fig 6.1(f) shows the received and wavelet images from receiver side

Fig:6.1(d),(e) and (f) .The results at receiver side.

6. CONCLUSION

The cryptographic algorithm alone is not a much secure way to be used for the data transmission. So a new method which combines cryptography and steganography is provided which gives much better option for data transmission. In this project a method to combine steganography (Least Significant Method) and cryptography (DES) is considered, so as to provide a more secure way for data transmission through any unsecured or public networks. To further increase the security of the data the encrypted text is not embedded in the image itself, instead it is embedded in the LL-subband of the wavelet transformed image.

7. REFERENCES

[1] William Stallings, Cryptography and Network Security, Principles and Practice, Third editionPearsonEducation, Singapore, 2003.

[2] Clair, Bryan. "Steganography: How to Send a Secret Message." 8 Nov. 2001

[3] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998. Pp. 32-47.

[4] C. C. Lin, and W. H. Tsai, "Secret Image Sharing with Steganography and Authentication," Journal of Systems and Software, 73 (3): 405-414, December 2004

[5] KafaRabah. Steganography - The Art of Hiding Data. Information Technology Journal 3 (3) - 2004.

[6] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

[7] Krenn, R., "Steganography and Steganalysis", http://www.Krenn.nl/univ/cry/steg/article.pdf

[8] R.J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Stegnography, IEEE Journal Selected Areas in Communications, 16 (4), pp. 474-481.

[9] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing," 2nd Ed., Pearson Education Pvt. Ltd, Indian Branch, 2003.

[10] Duane Hanselman and Bruce Littlefield, "Mastering MATLAB 7", Pearson Education, India.

[11] Daubechies Ingrid, "Ten Lectures on Wavelets," Society for Industrial and Applied Mathematics, 1992

[12] J. Fridrich, M. Long, "Steganalysis of LSB encoding in color images,"Multimedia and Expo, vol. 3 pp. 1279-1282, July 2000..

[13] R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice "International Workshop on Digital Watermarking, Seoul, October 2004.

[14] Hide & Seek: An Introduction to Stegnography: http:\\niels.xtdnet.nl/papers/practical.pdf.

[15] Y. Lee and L. Chen (2000) High capacity image steganographic model, IEE Proceedings on Vision, Image and Signal Processing, 147 (3), pp. 288-294.