Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Enhanced Security Technique for Steganography Using DCT and RSA

Shahana T*
M.Tech Student, Computer Science & Engineering, University of Calicut
K.M.C.T. College of Engineering, Calicut, Kerala, India

Abstract— Steganography transmits data by actually hiding the existence of the 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. During communication process LSB steganography based on Huffman encoding algorithm does not provide full security and good compression. So a secure DCT-based steganographic algorithm is proposed. This algorithm provides more security and compression by combining cryptography with DCT-steganography. Two 8 bit gray level images are used as cover image and secret image respectively. In this algorithm the cover image is transformed from spatial domain to frequency domain using DCT. Then an encrypted secret image is embedded in the cover image. A public–key encryption algorithm RSA is used in this paper. PSNR is used to measure the quality of stego images. Experimental results show that good PSNR value will be obtained. At the end an analysis is done and that shows that high PSNR value will be obtained when the size of secret image is less compared to the size of cover image.

Keywords— Steganography,frequency domain,DCT,RSA,Stego Image,PSNR

I. INTRODUCTION

With the development of internet technologies, digital media can be transmitted conveniently over the internet. In this situation image and message transmission have to face many problems. Therefore how to protect this transmission becomes an important issue. Privacy is another issue when digital communication is considered. Steganography and Cryptography are the two technologies related with security and privacy. Cryptography is a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Cryptography does not provide the existence of a message secret. To provide this steganography is used. Steganography is the art of hiding information that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing" (Greek words "stegos" meaning "cover" and "gratia" meaning "writing"). Steganography involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. The media with or without hidden information are called Stego Media and Cover Media, respectively. Steganography and Cryptography are cousins in the spycraft family.

The difference between Steganography and Cryptography is that the cryptography focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret. Steganography and cryptography both are ways for protecting information from unwanted parties. Two other technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property. In watermarking all of the instances of an object are “marked” in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property of owner to identify customers who break their licensing agreement by supplying the property to third parties.

In this paper proposes an image steganographic method. Steganography can be done for image, audio or video files. Here taking the images. An image is an array or a matrix of square pixels arranged in columns and rows. Images can be bilevel , grey or color images. Bilevel images have only two intensity values 0,1(black, white). Grey level image is 8-bit in which each picture element has an assigned intensity that ranges from 0 to 255. In the case of color images it is a 24-bit pixel which consists of red, green and blue colours(each will be 8-bit pixel). This paper implement the steganography for the grey level images. This grey level images are taken as the cover image and secret image. Steganography technique lihere uses Dct- steganography. In this type the cover image is transformed from spatial domain to frequency domain. Two dimensional DCT transformation is used. After appliying quantization and IDCT on DCT coefficients , the encrypted secret image is embedded . The secret image is encrypted using public key cryptography algorithm RSAng with compression a lossless compression Huffman coding is used in [1],[2],[3] is used.

The paper is organized as follows. Section II provides the Literature Survey, Section III provides the Proposed Steganography Method, and Section IV provides the Experimental Results.

II. LITERATURE SURVEY

When doing survey and analysis of current methods [5] different methods have so many advantage and disadvantages. . Different Steganography techniques discussed in [4] are spatial domain, frequency domain, and statistical or adaptive. In spatial secret image is embedded in the cover image without any modification to the cover image. That usually it is placed least significant bits of the cover image. But in frequency domain transformation technique such as DCT, DFT or DWT is used. Nowadays DFT is not used. In DCT secret image is placed in the low and mid frequency coefficients and In DWT it is embedded in the frequency sub bands. To provide security and compression different approaches have to be combined with steganography. When dealing with compression algorithms a lossless compression Huffman encoding is combined with LSB[1], DCT[2],and DWT[3]. In [1],[2],[3] hides a large amount of data with high security, good invisibility and no loss of secret message. When dealing with security issue different encryption algorithms are combined with steganographic technique. [6,7,8] different approaches used with LSB Steganography. In [6] In encryption phase, the data is embedded into carrier file which was protected with the password In [7] find the shared stego-key between the two communication parties by applying Diffie-Hellman Key exchange protocol, then encrypt the data using secret stego-key and then select the pixels by encryption process with the help of same secret stego- key to hide the data. Each selected pixel will be used to hide 8 bits of data by using LSB method. In [8] scheme uses RSA or Diffie Hellman algorithm to encrypt secret information. To provide higher security the secret information is encrypted first and encrypted ASCII value is converted in binary form In [9] the secret key will determine where to embed in the cover image. This work is done for the colour image. A steganography which combines the spatial and frequency domain method explained in [10]. In this method two outer cover images are used.

III. PROPOSED STEGANOGRAPHY METHOD

During communication processs LSB steganography based on Huffman encoding algorithm does not provide full security and good compression. So in this paper, we proposed a frequency domain steganography technique for hiding a large amount of data with high security, good invisibility and no loss of secret message. Two 8 bit gray level images are used as cover image and secret image respectively. The proposed scheme uses DCT steganography based on encryption. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image. First the cover image is divided in to 8-bit blocks. Then 2-D DCT convert the image blocks from spatial domain to frequency domain. Then using RSA encryption is appllied on secret image using RSA algorithm. This encrypted image has to be embedded in the DCT-coefficients of cover image. Then IDCT is performed and will get the stego image. To extract the secret image stego image is divided in to 8-bit blocks . Then 2D DCT is performed and encrypted secret image is taken and apply the decryption process and apply the IDCT will get the the original secret image. The schematic/ block diagram of the whole process is given in figure 1((a) and (b)).

A.Discrete Cosine Transform (DCT)

DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity.

Let I(x,y) denote an 8-bit grayscale cover-image with x = 1,2,…….,M1 and y = 1,2,…….,N1. This M1×N1 cover-image is divided into 8 × 8 blocks and two-dimensional (2-D) DCT is performed on each of L = M1×N1 / 64 blocks. The mathematical definition of DCT is:

$$F(u,v) = \frac{1}{4} C(u)C(v) \sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos\left[\frac{\pi(2x+1)u}{16}\right] \cos\left[\frac{\pi(2y+1)v}{16}\right]$$

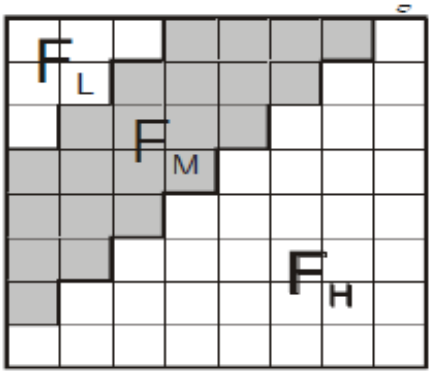
for u=0……...7, for v=0……7

$$where\ C(k) = \begin{cases} \frac{1}{\sqrt{2}} & for\ k = 0 \\ 1 & otherwise \end{cases}$$

The mathematical definition of IDCT is

$$f(x,y) = \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} C(u)C(v)F(u,v) \cos\left[\frac{\pi(2x+1)u}{16}\right] \cos\left[\frac{\pi(2y+1)v}{16}\right]$$

DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands which makes it easier to choose the band in which the secret image is to be inserted. Embedding the image in a middle frequency band does not scatter the secret information to most visual important parts of the image i.e. the low frequencies and also it do not over expose them to removal through compression and noise attacks where high frequency components are targeted . Although some of the steganography techniques embed the information in the DC component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of information into a DCT block. The middle-band frequencies (FM) of an 8*8 DCT block can be shown below in figure 2.1.DCT block consists of three frequency bands-Low frequency band (FL), High frequency band (FH), mid frequency band (FM). This system uses FM for embedding the watermark. Two locations Mi (u1, v1) and Mi (u2, v2) from the frequency band FM are chosen as the region for comparison.



B. Quantization

It is a lossy compression technique by compressing a range of values to a single quantum value. It reduces the number of colors required to represent a digital image, that makes it possible to reduce its file size. It constrains something from a relatively large or continuous set of values to a relatively small discrete set. The 8 x 8 block of DCT coefficients is compressed by quantization. Quantization is achieved by dividing each element in the DCT coefficient block by the corresponding value in the quantization matrix, and the result is rounded to the nearest integer. As eye is not able to discern the change high frequency components so these can be compressed to larger extent. Lower right side components of quantization matrix are of high value so that after quantization high frequency components become zero.

C. RSA Scheme

It is a best known and widely used public key cryptographic scheme. In public key cryptographic scheme two keys are used, one public key and one private key. One key used for encryption and one is used for decryption. Encryption is the process of transformin plain text to cipher text. Whereas decryption is the process of transforming from cipher text to plaintext. RSA is a lock cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n. In this system we are using the plaintext as the secret image. The image will have intensity values. If M is the set of intensity values to be encrypted, C is the result of encryption. RSA encryption and decryption process takes the following form which is explained in fig2 and fig3.

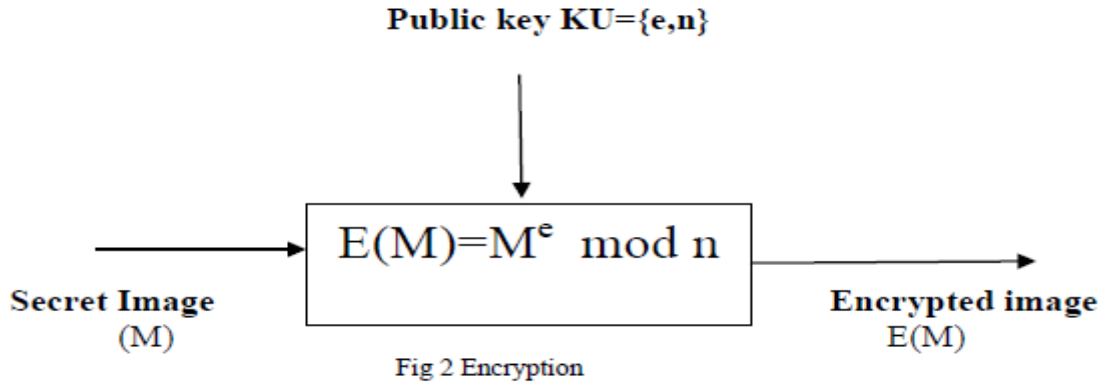


Fig 2 Encryption

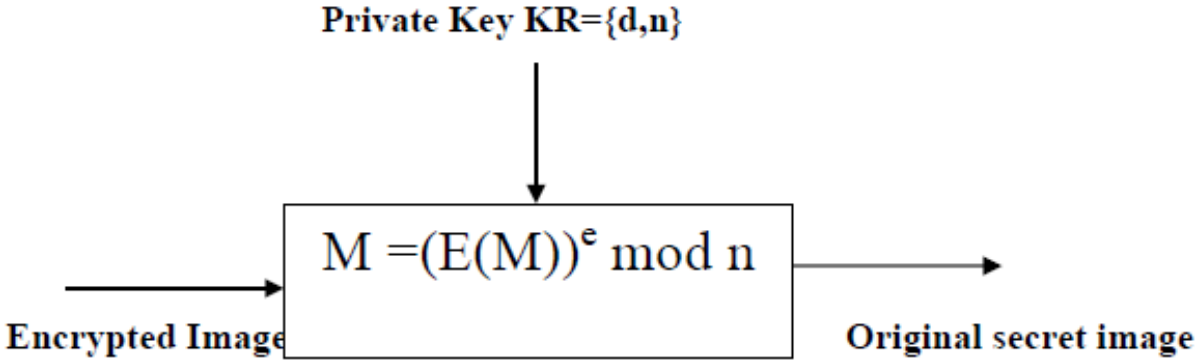


Fig3 Decryption

Title and RSA is a public key encryption algorithm with a public key of KU= {e,,n} and a private key of KR= {d, n}. Both encryption and decryption in RSA involve raising an integer to an integer power, mod n.

D. Embedding

Embedding is the process of placing secret image in to the cover image. In this system encrypted secret image is embedded in the mid-frequency DCT coefficients of the cover image. The result of embedding is a Stego image. This is explained in fig4.

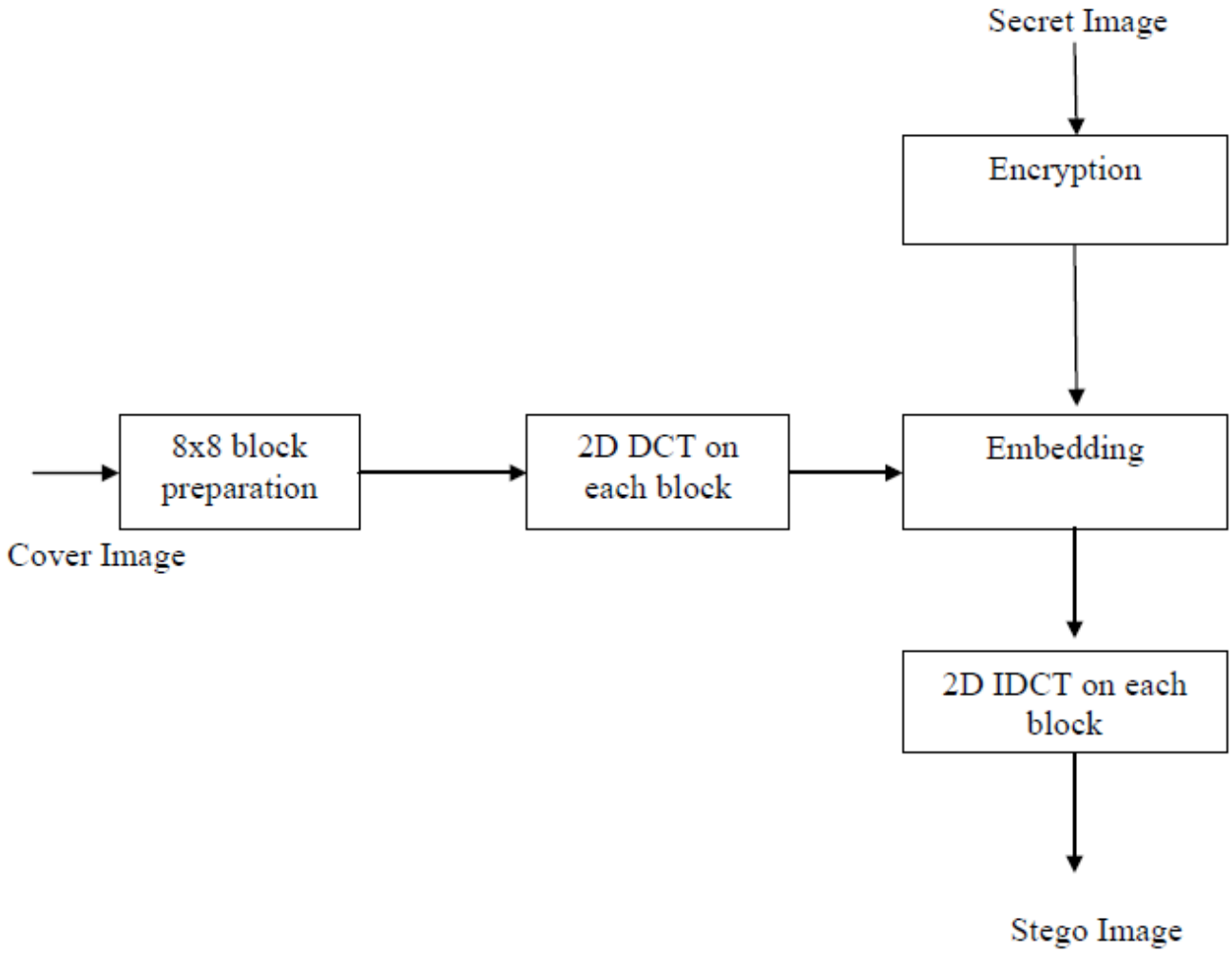


Fig 4 Embedding

Step 1:Load cover image and secret image.
Step2: Divide the cover image in to 8x8 blocks of pixels.
Step3: Transform the cover image from spatial domain to frequency using two dimensional DCT .
Step4: Quantize the DCT coefficients bydividing using factor in to the rounded value.
Step5: Encrypt the secret image using RSA algorithm.
Step7: Divide the encrypted image in to 8x8 blocks.
Step8: Embed this data in the mid DCT coefficients of cover image.
Step9: Apply two dimensional inverse DCT to view it in the spatial domain.

E. Extraction

Extraction is the process of taking secret image from stego image. In this system decrypted image is extracted. By applying RSA decryption on the encrypted image, will get the original secret image.

Step1:Read the Stego image.
Step2: Divide the stego image in to 8x8 blocks of pixels.
Step3: Transform the stego image from spatial to frequency domain by applying two dimensional DCT on each block
Step4: Quantize the DCT coefficients in to the rounded value.
Step6: Extract the encrypted image values from mid-frequency coefficients.
Step7: Decrypt the values using RSA algorithm.
Step8: Apply two dimensional inverse DCT to view the extracted image in the spatial domain.

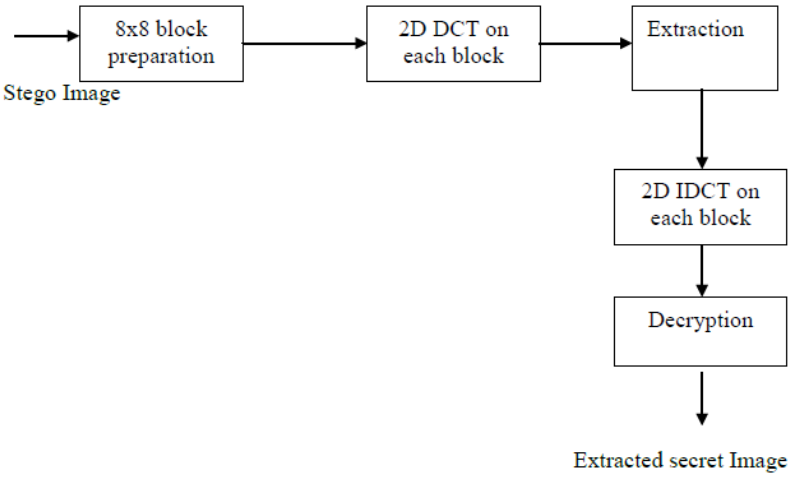


Fig5 Extraction

IV. Experimental Results

Some experiments are carried out to prove the efficiency of proposed algorithm. The measurement of the quality between the cover image f and stego-image g is done using PSNR (Peak Signal to Noise Ratio) value and the PSNR is defined as:

$$PSNR = 10 \times log(255^2/MSE)$$

Where

$$MSE = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\{f(x,y) - g(x,y)\}^2/N^2$$

f(x, y) and g(x, y) means the intensity value of pixel at position (x, y) of the cover image and stego image respectively. The PSNR is expressed in dB. Larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego image.

Figure 6(a),(d) shows the cover image and the secret image.

Fig 6(a)

Fig6(b)

Fig7(a)

Fig7(b)

Fig7(c)

Fig7(d)

Fig8(a)

Fig8(b)

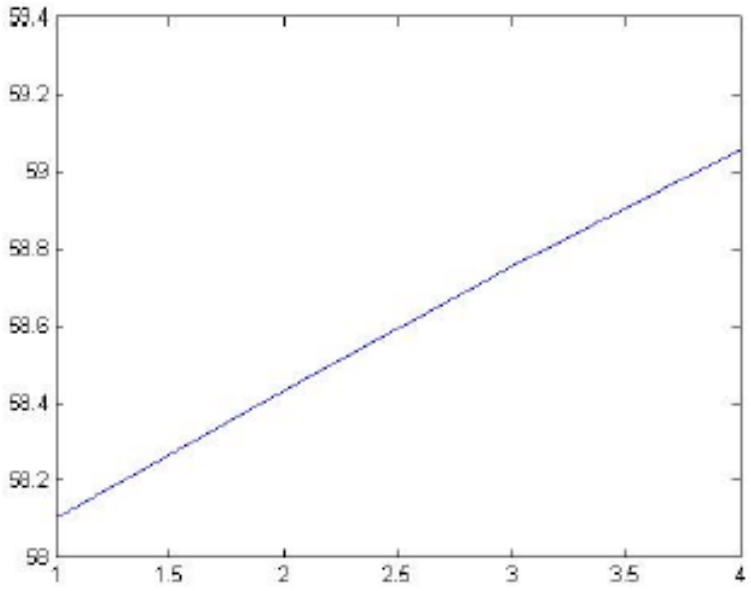
Fig9(a)

Fig9(b)

Fig9(c)

Fig9(d)

The graph shows that the PSNR of stego images becomes high when the size of secret image is less compared to the size of cover image.



IV. CONCLUSIONS

In this paper propose a DCT-steganography based on encryption. To provide high security steganography and cryptography are combined together. This system encrypts secret information before embedding it in the image. Steganography uses RSA algorithm for encryption and decryption. The encrypted image is placed in the mid frequency DCT coefficients of cover image, so that embedding done efficiently. According to the simulation results, the stego images of our proposed algorithm are almost identical to the cover images and it is very difficult to differentiate between them.. Better PSNR values will be obtained when doing this kind of steganography. Experimental results shows high PSNR values obtained when size of secret image is less compared to the size of cover image.

REFERENCES

[1] RigDas, Themrichon Tuithung," *A Novel Steganography Method for Image Based on Huffman Encoding*",2012 IEEE

[2] A. Nag, S. Biswas, D. Sarkar, P. P. Sarkar, "*A Novel Technique for Image Steganography Based on Block-DCT and Huffman Encoding*". International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010

[3] Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar," A *Novel Technique for Image Steganography Based on DWT and Huffman Encoding*" , International Journal of Computer Science and Security, (IJCSS)Volume 4

[4] Yam bern Jina Chanu, ThemrichonTuithung, Kh. Manglem Singh, *A Short Survey on Image Steganography and Steganalysis Techniques*, 2012 IEEE

[5] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt,*Digital Image Steganography: Survey and Analysis of Current Methods.*ELSEVIER Journal on Signal Processing 90 (2010) 727-752

[6] K.B.Raja', C.R.Chowdary2, Venugopal K R3, L.M.Patnaik , *A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images*,2005 IEEE

[7] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav , *Steganography Using Least Signicant Bit Algorithm* , International Journal of Engineering Research and Applications (IJERA) May-Jun 2012

[8] Shailender Gupta , Ankur Goyal , Bharat Bhushan ,*Information Hiding Using Least Significant Bit Steganography and Cryptography* , I.J.Modern Education and Computer Science, 2012

[9] Mohammad Ali Bani Younes , Aman Jantan , A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

[10] Gonzalez, R.C. and Woods, R.E., Digital Image Process in using MA TLAB, Pearson Education,Tndia,2006.

[11] Duane Hanselman and Bruce Littlefield, Mastering MATLAB@7 Pearson Education, India 2008.

[12] William Stallings,"Cryptography and Network Security, Principles and Practice ", Low Price Edition , Second Edition

