A Secure DCT Image Steganography based on Public-Key Cryptography

Shahana T

M.Tech student, Computer Science & Engineering,University of Calicut
KMCT College of Engineering
Calicut, Kerala, India

Abstract—**Steganography is the method of hiding information in a multimedia carrier. The carrier(cover) can be an image, audio or video. In this case image is taken as the carrier and the hidden information or secret information. So here dealing with image steganography. Gray level image is taken as both cover and secret images. This paper implements the steganography in frequency domain. A DCT transformation technique is used to convert the cover image from spatial to frequency domain. To provide more security public key cryptography is combined with steganography. A public key encryptionn algorithm RSA is used here. Secret image is encrypted before embedding in the cover image. PSNR value is calculated for both stego and extracted image. An analysis shows that high PSNR value is 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

The main issue arises during communication through insecure network is the security. Inorder to make this process secure, different techniques are used. Steganography and Cryptography are the two approaches that makes the communication secure. Steganography is a way of hiding the secret information in a medium. This makes the existence of an information secret. But cryptography is the way of scrambling the information. This makes the information secret, not the existence. Since both techniques are used for providing security and privacy, they are cousins in the spycraft family[3].

Another technique related with Steganography is Watermarking. In Watermarking owner’s property right for digital media(ie images, music,video and software) protected by some hidden watermark.

One of the main goal of Steganography communication in the secure manner, that is unwanted parties could not be able to see the hidden information. That is Steganalysis becomes a difficult process. Steganalysis is an art of deterring covert communications while avoiding affecting the innocent ones. Generally a steganographic system consists of cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, steganography gives a way in that someone cannot know the presence of the hidden message. There are two types of Steganography. Steganography in spatial domain, Steganography in frequency domain. In spatial domain secret image directly embedding in the cover image. Where as in frequency domain the cover image is transformed from spatial to frequency domain using some of the methods such as DCT,DFT or DWT method. Then the secret image is placed in the cover image in spatial domain. The image getting after this type of embedding process is called as the Stego image. A commonly used spatial domain technique is LSB Steganography. In this case the secret information stored in the least significant position of the cover image.

Cryptography are of two types. Private key and Public key cryptography. In private key, encryption and decryption uses same key . Whereas in public key encryption and decryption uses different keys(one private key, one public key).

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 level 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. Grey level images are taken as the cover image and secret image. Steganography technique here uses DCT- steganography. In this the cover image is transformed from spatial domain to frequency domain. Two dimensional DCT transformation is used. After applying quantization and IDCT on DCT coefficients , the encrypted secret image is embedded . The secret image is encrypted using public key cryptography algorithm RSA.

This paper is organized as follows. Section II provides the Literature Survey, Section III provides the Proposed Stegangraphy Method, and Section IV provides the Experimental Results and Section V provides Conclusion.

II LITERATURE SURVEY

When doing survey and analysis of current methods [5] different methods have so many advantages 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 in 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. Since Huffman encoding provides high compression the above paper does not shows better results. When dealing with security issue different encryption algorithms are combined with steganographic technique. In [6],[7],[8] different approaches combined with LSB Steganography. In [6] when considering the 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 to 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 STEGANAGRAPHY METHOD

In LSB steganography , there is direct embedding of data. This hiding can easily extracted by the unauthorized user. When combining with Huffman encoding ,this will not achieve full compression during the communication process. So a secure compressed steganography method is proposed. The method uses DCT- steganography with public key cryptographic algorithm RSA . In this method the cover image is transformed from spatial domain to frequency domain using 2D DCT. Then the secret image is encrypted using RSA algorithm and it is embedded inside the cover image to obtain the stego image. To extract the secret image apply 2D DCT on stego image and apply the decryption algorithm . The embedding and extraction process is explained in figure1 and figure 2.

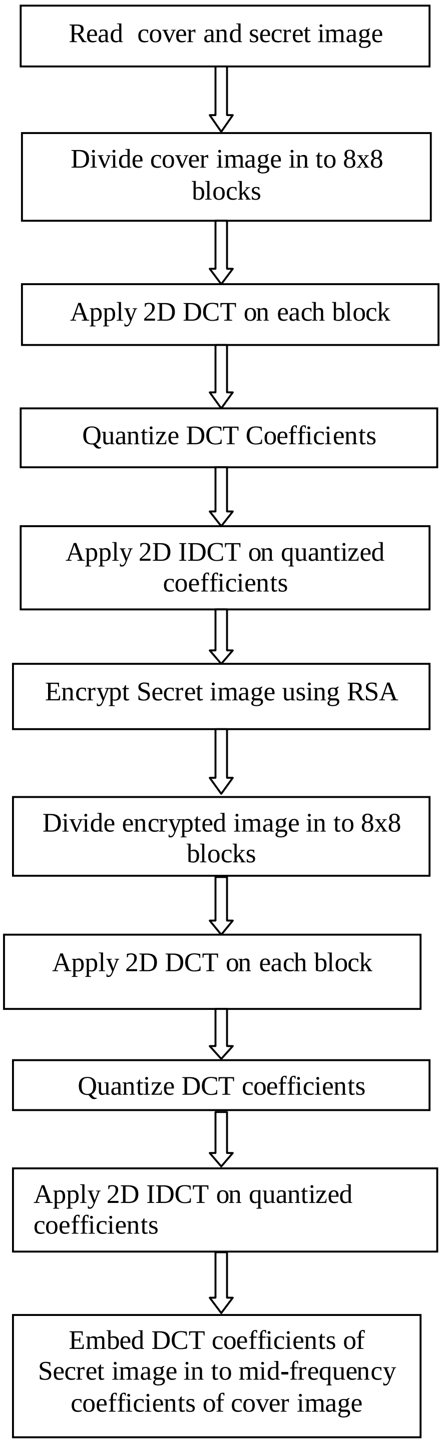
Read cover and secret image
Divide cover image in to 8x8 blocks
Apply 2D DCT on each block
Quantize DCT Coefficients
Apply 2D IDCT on quantized coefficients
Encrypt Secret image using RSA
Divide encrypted image in to 8x8 blocks
Apply 2D DCT on each block
Quantize DCT coefficients
Apply 2D IDCT on quantized coefficients
Embed DCT coefficients of Secret image in to mid-frequency coefficients of cover image

Figure 1 Embedding Process

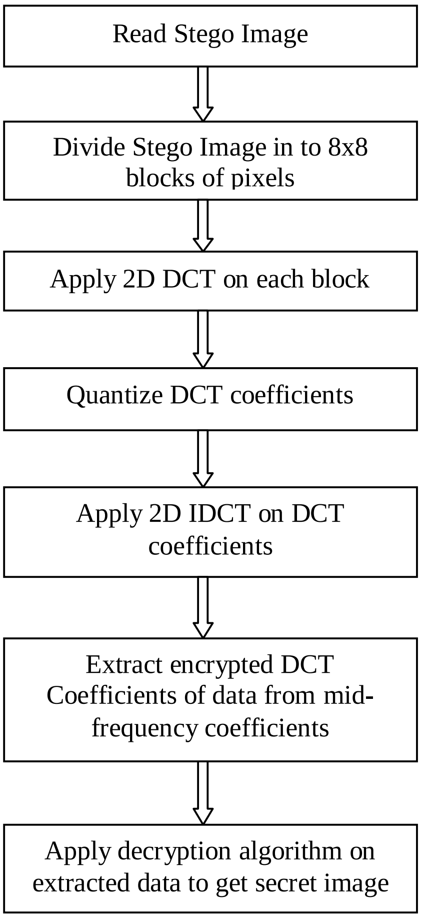
Read Stego Image
Divide Stego Image in to 8x8 blocks of pixels
Apply 2D DCT on each block
Quantize DCT coefficients
Apply 2D IDCT on DCT coefficients
Extract encrypted DCT Coefficients of data from mid-frequency coefficients
Apply decryption algorithm on extracted data to get secret image

Figure 2 Extraction Process

A. Discrete Cosine Transform (DCT)

The image of size M×N is divided into 8×8 blocks and two dimensional (2-D) DCT is performed on each block. The DCT is calculated using equation (1)

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

for u=0,...,7 and v=0,...,7

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

In DCT block lower frequency coefficients are at upper left positions and high frequency coefficients are lower right positions and mid frequency coefficients are in between them.

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 in 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. The quantized DCT coefficients matrix P is computed by equation (2)

$$P(u,v) = F(u,v)/Q(u,v) \qquad (2)$$

C. Inverse DCT

The two dimensional inverse DCT equation is defined in (3)

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

for x=0,...,7 and y=0,...,7 (3)

D. Encryption and Decryption

The encryption and decryption process consists of an algorithm and a key. Encryption converts from plaintext to cipher text. Where as decryption converts cipher text to plain text. Encryption can be classified in to two types. Symmetric encryption and Asymmetric encryption. In symmetric encryption a single key used for both encryption and decryption. In asymmetric encryption involves the use of two keys. An asymmetric encryption public key cryptography algorithm RSA is used here. The RSA scheme is a block cipher in which plaintext and ciphertext are integers between 0 and n-1 for some n. These integers represents the intensity values of the image.

E. 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.

F. Extraction

Extraction is the process of taking secret image is taken from stego image. In this system decrypted image is extracted.

Embedding Algorithm

Input: Cover image, Secret image
Output: Stego image

```
Algorithm:
Step 1: Read both cover and secret image.
Step2: Divide the cover image in to 8x8 blocks of pixels.
Step3: Apply two dimensional DCT on each 8x8 blocks of pixels to get 64 DCT coefficients.
Step4: Quantize the 64 DCT coefficients in to the rounded value.
Step5: Apply two dimensional IDCTon the quantized DCT coefficients.
Step6: Take mid frequency DCT coefficients of cover image for embedding.
Step6: Encrypt the secret image using RSA algorithm.
Step7: Divide the encrypted image in to 8x8 blocks of pixels.
Step8: Apply two dimensional DCT on each 8x8 blocks of pixels.
Step8: Embed the DCT coefficients of encrypted data in the mid frequency coefficients of cover image.
```

Extraction Algorithm:

Input: Stego image
Output: Extracted Secret Image

```
Algorithm:
Step1:Read the Stego image.
Step2: Divide the stego image in to 8x8 blocks.
Step3: Apply two dimensional DCT on each block
Step4: Quantize the DCT coefficients in to the rounded value.
Step5: Apply two dimensional IDCT on each block.
Step6: Extract the encrypted image values from mid-frequency coefficients.
Step7: Decrypt the values using RSA algorithm.
```

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 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. All the simulation has been done using the MATLAB 7 program on Windows 7 platform.

Table I shows the PSNR values between cover image and stego image and between secret image and extracted image.

TABLE I

Secret Image: Wom1

Cover image	PSNR between Cover image and Stego image
Fce5	63.543
Fce6	61.433
Kiw1	62.356
Scr1	63.654

Figure 3(a)-(d) shows the cover images and 3(e) shows the secret image.

Fig. 3(a) fce5

Fig. 3(b) fce6

Fig.3(c) kiw1

Fig. 3(d) scr1

Fig.3(c) wom1

Figure 4(a)-(d) shows the the stego images and figure 4(e) shows the extracted image

Table II shows the PSNR values for different stego images when the cover image kept constant and secret images are of different. From this table high PSNR value will be obtained when the size of secret image is less compared to the size of cover image. That is the good advantage of this proposed system.

Fig. 4(a) fce5

Fig. 4(b) fce6

Fig.4(c) kiw1

Fig. 4(d) scr1

Fig.4(e) wom1

TABLE II

Cover Image: Kiwl of size 515x393

Secret Image	PSNR between cover image and stego image	Size of image
scr1	46.765	507x384
Fce5	55.659	306x341
Fce6	56.765	316x252
wom1	63.765	256x256

V 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 in the image. Steganography uses RSA algorithm for encryption and decryption. 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 get when compared with LSB steganography with Huffman coding. Experimental results shows high PSNR values obtained when the 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 Processing using MATLAB*, Pearson Education,India,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.