International Journal of Advanced Research and Development
ISSN: 2455-4030, Impact Factor: RJIF 5.24
www.newresearchjournal.com/advanced
Volume 1; Issue 6; June 2016; Page No. 17-20

Compression of frequency domain based Stego-Image for swift transmission

Sudhanshu Garg, Farhan Khan

Guided By Anitha J. (Assistant Professor) Department of Computer Science and Engineering SRM, Chennai, India

Abstract
Network is a group of many computer systems connected together. Computer networks are of many types, which includes: local-area networks (LANs), wide-area networks (WANs) metropolitan area networks (MANS).Network security subsist of the policies adopted to prohibit and monitor unauthorized access, misuse, modification, or denial of network-accessible resources and a computer network. Security of network includes the authorization of access to data in a network, which is controlled by the network administrator. In this project, we send the data from sender to receiver securely by using steganography method. Steganography is used to hide the data inside the image. In existing system, the secret data which is embedded inside the cover image could make the resulting image very large in size, so it consumes more time for transmission. But in this proposed system, user can compress the data which is to be shared which will reduce the transmission time for sending the data from sender to receiver. Through this method of compression, the total time required for sending the data can be remarkably reduced. The main theme of this project is to transmit the data securely in the network. The user can hide the data in the image which he wants to share securely and also he can compress the data, so the files size will be reduced and this will increase the transmission speed of the data and hence can save a lot of time.

Keywords: Steganography, LSB, Edge encryption, frequency domain, DCT, Stego Image.

1. Introduction
Steganography is an age old method to hide data. But with the advent in media technology, many different ways have been set down for the same. We can apply this method in image, video, text and audio. The advancement in Information Technology has made it necessary for encrypting crucial data to make it reversible to the desired one. Steganography is correspondent to cryptography, where it aims at hiding the existence of a message rather than making the message illegible through encryption. Thus Steganographic applications are essential where public interference is to be prohibited and keep the original data being uncorrupted. This paper proposes an image/text steganography method. Steganography can be done for image, audio or video files. Here considering the images. An image is a matrix of square pixels arranged in rows and columns. Images can be bit-level, grey or colour images. Bit-level images have only two intensity values 0, 1(black, white). Grey level image is an 8-bit in which each picture element has a given intensity that has a range from 0 to 255. In the case of colour images it is a 24-bit pixel which consists of red, green and blue colors (each will be 8-bit pixel).Here we implement the steganography for the grey level images. This grey level images are selected as the secret image and cover image. Steganography technique here uses DCT- steganography. In this type, the cover image is transformed from spatial domain to frequency domain with DCT-II. After applying DCT (Discrete cosine transform), the encrypted secret image/data is embedded. And finally, the image is compressed with the Quantization technique.

2. Literature Survey
When doing survey and analysis of current strategies [5]. we find that, totally different strategies have such a big amount of pros and cons. totally different Steganography techniques mentioned in [4]. are abstraction domain, spatial domain and applied math or adaptation technique. In abstraction, secret image is embedded within the cowl image with none modification to the quilt image. Sometimes it is placed at the least important bits of the quilt image. However in frequency domain transformation technique like DCT, DFT or DWT is employed. Today DFT isn't used. In DCT secret image is placed within the low and middle frequency coefficients and In DWT it's embedded within the frequency sub bands. To produce security and compression totally different approaches need to be combined with steganography. Once handling compression algorithms a lossless compression Huffman encryption is combined with LSB [1]. DCT [2] and DWT [3]. In [1, 2, 3] hides an oversized quantity of information with high security, sensible invisibleness and no loss of secret message. Once handling security issue totally different encoding algorithms are combined with Steganographic technique [6] totally different approaches are used with LSB Steganography. In [6]. In encoding section, the information is embedded into carrier file that was protected with the word we notice that the shared stego-key between the 2 victimisation secret stego-key then choose the pixels by encoding method with the assistance of same secret stego- key to cover the information. Every selected component are wont to hide eight bits of information by victimisation LSB methodology. In theme uses RSA or Diffie dramatist algorithmic rule to write in code secret information to produce higher security the key info is encrypted 1st and encrypted ASCII worth is reborn in binary kind In the key can verify wherever to plant within the cowl image. This work is finished for the colour image. A steganography which mixes the abstraction and frequency domain methodology explained in. During this methodology 2 outer cowl pictures are used

3. Proposed Steganography Method During the process of communication, LSB (Least Significant Bit) steganography

based on only Huffman encoding algorithm does not provide good compression and full security. Here, we introduce a method of frequency domain steganography technique for hiding a hefty amount of data with good security and no loss of secret message. Two eight-bit gray level images are used as secret image and cover image correspondingly. The introduced scheme uses DCT (Discrete Cosine Transform) based encryption technique. The essential idea to cover information within the frequency domain is to change the magnitude of all of the DCT coefficients of selected cover image. First the selected cover image is divided into 8-bit blocks, then 2-D DCT convert the image blocks to frequency domain from spatial domain. This encrypted image/data has to be planted in the DCT-coefficients of the selected cover image. Then IDCT is performed to get the stego image. Now, to extract the secret image/data, stego image is divided into 8-bit blocks. Then 2-D DCT is applied and encrypted secret image/data is taken out, then the decryption process is applied and then the IDCT is applied. Through this we get the original secret image/data.

A. Discrete Cosine Transform (DCT)

DCT is a simple orthogonal transform for image processing and signal processing which has pros like high compression ratio, good information integration property and good synthetic effect of computation complexity.

Let I(x, y) denote a 8-bit greyscale cover image with x = 1,2,…….,M1 and y = 1,2,…….,N1. This M1×N1 cover-image is spitted into 8 × 8 blocks and 2-D DCT is performed on each of L = M1×N1 / 64 blocks. This can be mathematically expressed as:

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

for u=0……..7 and for v=0……7

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

The mathematical expression of IDCT is

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

B. Quantization

Quantization is a compression technique which is done by compressing a range of values to a single quantum value. It reduces the number of colors needed to represent a digital image, which makes it possible to reduce the size of the file. It constrains something from a comparatively large or continuous set of values to a relatively small discrete set. The 8 x 8 bit blocks of DCT coefficients is compressed through this process. Quantization is reached by dividing each element present in the DCT coefficient block by the corresponding value in the quantization matrix/table, after that the result is rounded to the nearest integer. Our eye is incapable to recognize the variation in the high frequency components so they can be compressed to a huge extent. The lower right side elements of quantization matrix has high value, so that post quantization the high frequency components will become zero.

C. Huffman encoding and Huffman table (HT)

Before embedding the data inside the cover image, it is first encoded using Huffman coding. Huffman codes are the codes which map one symbol to one code word. The Huffman encoding algorithm is a general compression algorithm, and the frequency of every letter is used to compress the data. The idea behind the algorithm is that if we have some letters that are more frequent than others, it is good to use fewer bits to encode those letters as compared to the less frequent occurring letters. Huffman table (HT) contains binary codes to each occurring value. Huffman table should be same in the decoder and the encoder. Therefore the Huffman table should be sent along with the compressed image data.

D. 8-bit block preparation

Huffman code H is decomposed into the 8-bits blocks B. Let's take the length of Huffman encoded bits stream to be LH. Thus if LH is not divisible by 8, then last block contains r = LH % 8 number of bits (% is used as modulo operator).

E. Embedding

Embedding is the process of planting the secret image into the cover image. In this system, encrypted secret image is embedded in the mid-frequency DCT coefficients of the image we selected as cover. The result of embedding is a Stego image.

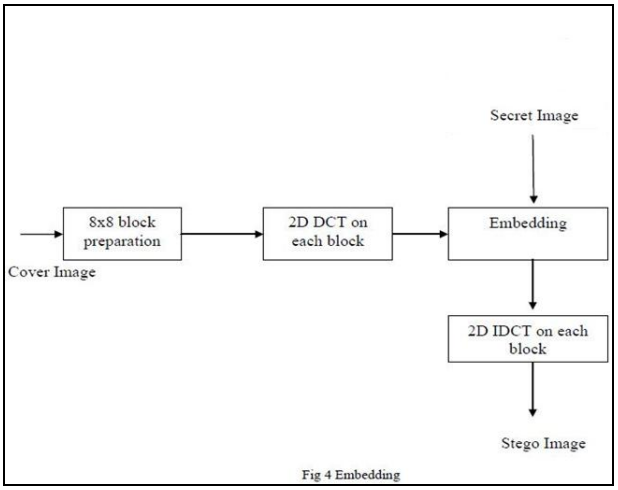

Fig 1: This is explained in

We proposed the secret message/image embedding scheme which comprises of the following six steps:

Step 1: To divide the cover image in to 8x8 blocks of pixels and transform the cover image from spatial domain to frequency using 2-D DCT (discrete cosine transform).

Step 2: Perform Huffman encoding on the 2-D secret image S of size M2 × N2 to convert it into a 1-D bits stream H.

Step 3: Divide the Huffman code H in to 8x8 blocks B.

Step 4: The least significant bit (LSB) of all of the DCT coefficients inside 8×8 block is changed into a bit taken from each 8 bit block B from left to right. The method is as follows:

For k=1; k<=1; k=k+1

LSB $((F(u,v))_2)$ B(k);

Where, B (k) is the k^{th} bit from left to right of a block B and $(F(u,v)_2)$ is the DCT coefficient in binary form.

Step 5: Quantize the DCT coefficients by dividing, using factor, into the rounded value.

Step 6: Now using the inverse DCT (IDCT) to view it in the spatial domain.

F. Extraction

Extraction is the procedure of taking out the secret image from stego image. The stego-image is received in spatial domain. DCT is performed on the stego-image using the same block of size 8 × 8 to transform the stego-image to frequency domain from spatial domain. The size of the encoded bit stream of secret message/image are extracted along with the Huffman table of the secret message/image. The given diagram of the extracting process is in figure 5 and the extracting algorithm follows it:

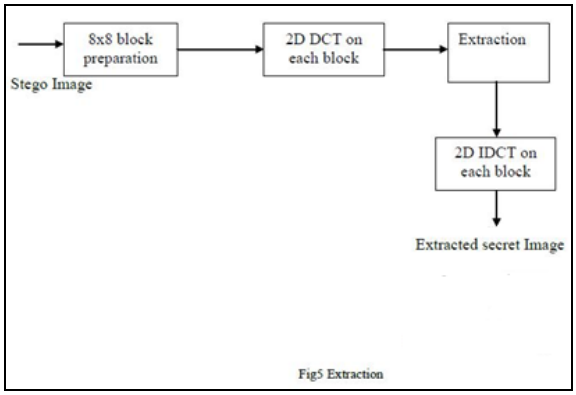

Fig 2

Step 1: Recreate the image by multiplying the factors to form the coefficient.

Step 2: Divide the stego-image into block size of 8×8 and use DCT on each of the blocks of the stego-image.

Step 3: The size of the bit stream is taken out from the 1^{st} 8 × 8 DCT block, by collecting the least significant bits of all the DCT coefficients within the 1^{st} 8×8 block. After that, all the least significant bits of all of the DCT coefficients inside 8×8 block (excluding the first) are gathered and added to a 1-D array.

Step 4: Apply 2-D inverse DCT to view the extracted image in the spatial domain.

4. Experimental Results

Few experiments are carried out to check the efficiency of our 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 $MSE = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (f(x,y) - g(x,y))^2 / N^2$

Where,

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

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

Fig 3: (a) Lenna

Fig 3: (b) Secret Image

The table shows that the PSNR of stego images becomes high when the proposed algorithm is used than compared to the Existing algorithm.

	Modified Side Match		
Cover Images	Size(Kb)	Capacity(bits)	PSNR(dB)
Lenna	248	168,289	43.64
	Proposed Method		
	Size(Kb)	Capacity(bits)	PSNR(dB)
	246	299,520	48.48

Figure 7 (a) shows the resulted stego-images of the proposed methods.

(a) Lenna

Fig 4: Stego image of the proposed method

5. Conclusions

This paper proposes a steganography process in the frequency domain which improves security and quality of the image greatly as compared to the existing systems and the algorithms which are usually used in the spatial domain steganography. As compared with the results obtained from PSNR values, proposed method has a better outcome as compared to the other methods and there is not much difference between the stego images and the original images. Additionally, this algorithm provides extra 3 layers of security through the transformation (DCT and Inverse DCT) of cover images and Huffman encoding of secret text/image. The need of toughness in image steganography field is not requested as powerful as it is in watermarking field. As a product, image steganography method usually ignores the basic demand of toughness. In our proposed method the embedding process is concealed underneath the transformation i.e. DCT and inverse DCT. All these operations and Huffman encoding of secret text/image keeps the data away from destroyed or stolen from attackers and hence the proposed method may be better against unwanted attacks. Steganography will be a major interest for researchers because of its uses in various fields. Selecting a new path in Image Processing, Steganography has led open a new path for researchers and developers to find a new ways of security.

6. References

1. DES Encryption Standard (DES), National Bureau of Standard (U.S). Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA, 1997.
2. Daemen J, Rijmen V. Rijndael the Advanced Encryption Standard, Dr. Dobb's Journal. 2001.
3. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communication of the ACM, 1978, 120-126.
4. Pfitzmann B. Information hiding terminology, Proc. First Workshop of Information Hiding Proceedings, Cambridge, U.K Lecture Notes in Computer Science, 1996; 1174:347-350.
5. Wang H, Wang S. Cyber warfare: Steganography vs. Steganalysis, Communications of the ACM, 2004; 47-10.
6. Jamil T. Steganography: The art of hiding information is plain sight, IEEE Potentials, 1999; 18-01.