Information Security Technique in Frequency Domain

*1Thekra Abbas, 2Zou Beiji, 3Maan Younus Abdullah
1 2School of Information Science and Engineering, Central South University, Changsha 410083, China, thekra.abbas@yahoo.com
3College of computer sciences and mathematics University of Mosul, Iraq, maan916031@yahoo.com

Abstract
There have been many hidden communication techniques proposed in the last few years. The focus of this development was given to steganography to build such techniques. This paper presents a novel technique for Image steganography based on a frequency domain, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain, and then Huffman encoding is performed on the secret messages/images before it is embedded in the frequency domain. The number of payload bits \( L \) is embedded into the DCT coefficient based on the DCT coefficient value of cover image in order to maximize the hiding capacity. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing algorithm.

Keywords: Steganography, Hidden communication techniques, Frequency domain, DCT, Huffman coding, Payload (MSB), Peak Signal to Noise Ratio (PSNR) Information hiding.

1. Introduction
Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as 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. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

The outcome of the steganographic system is a stego-media which is perceptually indiscernible compare to the cover media, but with embedded hidden data. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography[1,2]. Shown in Fig.1 are the different embodiment disciplines of information hiding.

Some techniques attempt to protect the embedded message by scrambling the messages bits before being hidden. Liu et al. [3] scramble the secret message by adding to it a pseudo-random sequence generated by a shared secret key. The authors utilize the DWT coefficients to hide the message [4]. Marvel et al. [5] use a similar idea to protect the embedded message. The spread spectrum communication, error correction coding, and image processing are combined to present their technique. Both these methods suffer from the key-distribution problem.


Another way to protect the embedded message is to randomize, or permute, the cover image using the stego-key before the embedding process. Pan et al., [10] propose to divide the image into sub-blocks. These blocks are ranked based on a specific pattern matching method so that the higher ranked block is the most suitable for data embedding. Tseng et al. [11] propose a scheme that is able to conceal critical messages into binary images. In [12] a new spatial domain steganography technique was proposed.
All these methods require that the sender and the receiver to agree upon the shared stego-key in advance.

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 where the numbers of payload bits \( L \) are embedded into the DCT coefficient of cover image based on the DCT coefficient value in order to maximize the hiding capacity. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of cover image. The 2-D DCT convert the image blocks from spatial domain to frequency domain. Our proposed method is robust against attack, it improves both image quality and security and increases embedding capacity.

The paper is organized into following sections. Section 2 is steganography methods. Discrete cosine transform is explained in section 3. In section 4 Huffman coding is described. The model of the proposed method is explained in section 5. In section 6 algorithms for the proposed method are described. Section 7 the simulation results. Finally, some conclusions and discussions are given in section 8.

2. Steganography methods

Steganography can be accomplished by simply feeding into a Windows OS command. The idea behind this is to abuse the recognition of EOF (End of file). In other words, our message reveals itself after displaying some data.

Another implementation of steganography is to append hidden data into the image’s extended file information (EXIF), which is a standard used by digital camera manufacturers to store information in the image file, such as, the make and model of a camera, the time the picture was taken and digitized, there solution of the image, exposure time, and the focal length[13].

In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs [14]. It is apparent to an observer that Fig. 2 concludes that there is a trade-off between the payload and the cover image distortion; however the payload, (embedding up to the 1st, 2nd, 3rd, or 4th LSB) is analogous with respect to the recovered embedded image. For instance, Fig.2(f) (recovered from embedding into 4 LSBs) is a good estimate of the hidden image of Fig. 2(a) but produces noticeable artifacts as shown in Fig.2(d). On the other hand Fig.2 (e), recovered from embedding into 1st LSB, trades bad quality with an almost identical carrier to the original (compare Fig. 2(c) with Fig. 2(b)).
Information Security Technique in Frequency Domain
Thekra Abbas, Zou Beiji, Maan Younus Abdullah

3. Discrete Cosine Transform (DCT)

The LSB embedding mechanism is actually a big achievement although it is perfect in not deceiving the VHS, its weak resistance to attacks until the researchers applied it within the frequency domain. DCT is used to transform the image from a spatial domain to frequency domain [18]. The description of the two-dimensional DCT for an input image $f(x,y)$ and an output image $F(u,v)$ is calculated as shown in equation (1):

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos \left( \frac{\pi (2x+1) u}{2M} \right) \cos \left( \frac{\pi (2y+1) v}{2N} \right)$$
Inverse DCT is calculated as shown in equation (2):

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

For \( u = 0, \ldots, 7 \) and \( y = 0, \ldots, 7 \)

Where \( C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k=0 \\ 1 & \text{otherwise} \end{cases} \)

If \( M, N \) are the dimensions of the input image then \( x, y \) are variables ranging from 0 to \( M-1 \) and 0 to \( N-1 \) respectively.

4. Huffman encoding

Before embedding the secret image into the cover image, it is first encoded using Huffman coding. Huffman codes are optimal codes that map one symbol to one code word [19].

![Huffman Encoding Technique]

For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D \( M \times N \) image is converted to a 1-D bits stream with length \( LH < M \times N \). Huffman table (HT) contains binary codes to each intensity value. Huffman table must be same in both the encoder and the decoder. Thus the Huffman table must be sent to the decoder along with the compressed image data. Huffman code \( H \) is decomposed into 8-bits blocks \( B \). Let the length of Huffman encoded bits stream be \( LH \) [20]. Thus if \( LH \) is not divisible by 8, then last block contains \( r = LH \% 8 \) number of bits (% is used as modulo operator).

5. MODEL

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section evaluation parameters and proposed embedding and retrieval techniques are discussed.

5.1 Evaluation Parameters
5.1.1 Peak Signal to Noise Ratio (PSNR)

It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage, is calculated as shown in equation (3), as a performance measurement for image distortion. It is defined as:

$$\text{PSNR} = 10 \times \log_{10} \left( \frac{C_{\text{max}}^2}{\text{MSE}} \right)$$  \hspace{1cm} (3)$$

Where MSE denotes mean square error which is given as:

$$\text{MSE} = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$$  \hspace{1cm} (4)$$

Where x and y are the image coordinates, M and N are the dimensions of the image, $S_{xy}$ is the generated stegoimage and $C_{xy}$ is the cover image. Also $C_{\text{max}}^2$ holds the maximum value in the image, for example:

$$C_{\text{max}}^2 \leq \begin{cases} 1 & , \quad \text{double precision} \\ 255 & , \quad \text{unit 8 bit} \end{cases}$$

5.1.2 Capacity

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage.

5.2 Proposed Embedding Technique

Firstly a gray level image of size M×N is divided into no joint 8 × 8 blocks and a two dimensional Discrete Cosine Transform(2-d DCT) is performed on each of the P = MN / 64 blocks. The payload is embedded into the cover image by segmentation, DCT and consistent bit length L. The embedding technique is shown in Fig.5 and illustrated in the following steps:

**STEP 1:** Cover Image: The cover image is color or gray scale of any size and format. If the cover image is color then convert into gray scale image and corresponding pixel intensity values.

**STEP 2:** Pixel Management: The gray scale cover image pixel intensity varies from zero to 255. During the payload embedding process the intensity values of cover image may exceed lower and higher level limits which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240 instead of zero and 255.

**STEP 3:** Segmentation: The cover image is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload.

**STEP 4:** 2D-DCT: Transform each 8x8 matrix into frequency domain using 2D-DCT. Using DCT on 8*8 sub blocks has an advantage of less computation time for embedding as well as security to payload increases compared to applying DCT to whole cover image.

**STEP 5:** Consistent bit length L: Determines the number of LSBs of each DCT coefficients (C0) of cover image that can be used to hide the payload MSB bits depending on each coefficient value. The conditions to determine L also serves as secret key to retrieve the payload at the destination.

**STEP 6:** Secret image: Perform Huffman encoding on the 2-D secret image S of size M2 × N2 to convert it into a 1-D bits stream and calculate the size of encoded bit stream in bits. Huffman code H is decomposed into 8-bit blocks B.

**STEP 7:** Embedding: the payload bits are embedded into the DCT coefficients of the cover image coherently based on the coefficients’ values.

---

Information Security Technique in Frequency Domain
Thekra Abbas, Zou Beiji, Maan Younus Abdullah

283
STEP 8: IDCT: The stegoimage in the transform domain is converted to the spatial domain by applying IDCT. The stegoimage obtained is similar to the cover image and the difference is not perceptible by the human eye. This image is transmitted to the destination over the open channel.

![Block Diagram of Embedding Technique](image-url)

**Figure 5.** Block Diagram of Embedding Technique

5.3 Retrieval Technique

The payload is retrieved from the stegoimage by adapting reverse process of embedding technique as shown in Fig. 6.

STEP 1: Stegoimage: The stegoimage is received in special domain.

STEP 2: Segmentation: The stegoimage is segmented into 8x8 blocks to ensure proper retrieval of payload.

STEP 3: 2D-DCT: The 8x8 sub blocks of stegoimage are transformed into frequency domain to generate DCT coefficients using 2D-DCT.

STEP 4: Bit length L: At the receiver L is determined based on the DCT coefficient values similar to the conditions of embedding technique. A sparse matrix is initially taken as payload output matrix. The payload bits are extracted into this output matrix based on the value of L to get back the payload.

STEP 5: The size of the encoded bit stream and the encoded bit stream of secret image are extracted along with the Huffman table of the secret image.

6. Algorithm
6.1 Embedding Algorithm

Input: An M1×N1 carrier image and a secret message/image.
Output: A stego-image.

1. A cover image of any size and format is considered and is converted to gray scale.
2. Apply pixel management to the cover image, to avoid overflow and underflow.
3. Obtain Huffman table of secret message/image.
4. Find the Huffman encoded binary bit stream of secret-image by applying Huffman encoding technique using Huffman table obtained in step 1.
5. Calculate size of encoded bit stream in bits.
6. Divide the carrier image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the cover image.
7. Repeat for bit obtained in step 5
   (a) Calculate the length L of each DCT coefficient according to the conditions:
      If co ≥ 2^5; L=5
      If 2^4 ≤ co ≤ 2^5; L=4
      If 2^3 ≤ co ≤ 2^4; L=3
      Else L=2
   (b) Insert the bits into the LSBs positions with the length L of each DCT Coefficient of first 8×8 block found in step 6.
8. Decompose the encoded bit stream of secret message/image obtained in step 2 into 1-D blocks of size 8 bits.
9. Repeat for each 8-bit blocks obtained in step 8
   (a) Change the LSBs positions with length L of each DCT coefficient of each 8×8 Block (excluding the first) found in step 6 using the same condition in step (7-a) To bits taken from left (LSBs) to right (MSBs) from each 8 bit block B.
10. Repeat for each bit of the Huffman table
    (a) Insert the bits into LSBs positions of each DCT coefficient using the same Condition in step (7-a)
11. Apply inverse DCT using identical block size.
12. End.
6.2 Retrieving Algorithm

Input: An $M1 \times N1$ Stego-image.
Output: Secret image.
1. Divide the stegoimage into non overlapping blocks of size $8 \times 8$ and apply DCT on each of the blocks of the stegoimage.
2. The size of the encoded bit stream is extracted from first $8 \times 8$ DCT block by calculating $L$ of the DCT coefficients inside the first $8 \times 8$ block (similar to the procedure adaptive in the embedding technique).
3. The payload length $L$ LSB of all the DCT coefficients inside $8 \times 8$ blocks (excluding the first) are collected and added to a 1-d array.
4. Repeat step 3 until the size of the 1D array becomes equal to the size extracted in step 2.
5. Construct the Huffman table by extracting the LSBs positions with length $L$ of all of the DCT coefficients inside $8 \times 8$ blocks excluding the first block and the block mentioned in step 3.
6. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.
7. End.

7. Simulation Results

In this section, some experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 8 program on Windows XP platform. A set of 8-bit grayscale images of size $512 \times 512$ are used as the cover-image to form the stegoimage. As shown in Fig.7, the two cover images (lenna, baboon) are considered into which the payload Cameraman (CM) image is hidden to generate stego-images. At the recipient end, the payload is extracted from the stegoimages; the advantage of using frequency domain image in steganography is that, the alteration of the content of the image will not easily cause visual artifact that arises suspicion as compared to spatial domain image.
Table 1 show that the Maximum Hiding Capacity (MHC) in terms of bits as well as the PSNR between the cover image and stegoimage is tabulated for existing algorithms (SDCTH) [21], (ASIWT) [22] and the proposed method. It is observed that the PSNR is improved around 25% in the proposed algorithm compared to the existing frequency domain algorithms.

Table 1. Capacity and PSNR of SDCTH, ASIWT and the proposed method

<table>
<thead>
<tr>
<th>Cover Images</th>
<th>SDCTH[21]</th>
<th>ASIWT [22]</th>
<th>proposed Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Capacity MHC (bits)</td>
<td>PSNR (dB)</td>
<td>Capacity MHC (bits)</td>
</tr>
<tr>
<td>(Lena &amp; CM)</td>
<td>299520</td>
<td>50.48</td>
<td>986408</td>
</tr>
<tr>
<td>(Baboon &amp; CM)</td>
<td>299520</td>
<td>50.28</td>
<td>1008593</td>
</tr>
</tbody>
</table>

Differences between original histogram and a histogram with embedded message bits using DCTCR technique [14] are illustrated in Fig.8 histogram (e). These differences can easily be detected by statistical attack. In this proposed method the differences becomes minimal as illustrated in Fig.8 histogram (d). The quality of the stegoimage which is determined by PSNR not only depends on the algorithm but also on the images used. The Lena as cover image gives higher PSNR compared to the cover image Baboon.

Frequency of occurrence
8. Conclusions

In this paper, we propose a steganography process in frequency domain. According to the simulation results the stego-images of our method are almost identical to other methods’ stegoimages and it is difficult to differentiate between them and the original images.

The performance results in terms of PSNR for different kinds of images and dimensions are better in the proposed algorithm in addition the data in the cover image are modified without deteriorating the integrity of the cover image.

The quality of the stegoimage which is determined by PSNR not only depends on the algorithm but also on the images used. The original LSBs information may have statistical properties, so changing some LSBs could result in the loss of those properties. Thus, we have to embed the message mimicking the characteristics of the cover bits.

Our proposed algorithm also provides four layers of security by means of transformation (DCT and Inverse DCT) of cover image, the MSB bits of payload are embedded into each DCT coefficients of cover image based on the coefficient value which is used to determine the length L, the fourth layer is a Huffman encoding of secret image. These layers keep the images away from being stolen, distorted by unintended users and hence the proposed method may be more robust against brute force attack.

9 Acknowledgements

This research is supported by National Natural Science Funds of China (No.60970098, No.60803024, No.60903136, and No.61173122), Major Program of National Natural Science Foundation of China (No.90715043), Hunan Provincial Natural Science Foundation of China (No.11JJ3067), and Fundamental Research Funds for the Central Universities (No.201021200062).
10 References