International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 08, August-2015

A Data Hiding Technique using Block-DCT

Rosemary Koikara
Student/Department of CSE
Christ University, Bangalore, India

Mausumi Goswami
Assistant Professor/Department of CSE
Christ University, Bangalore, India

***Abstract*—In this paper we are concerned with securing a secret image in such a way that only the sender and receiver know that a secret has been hidden in an image. Data hiding techniques are generally used to carry out this task. In this paper a data hiding scheme in the frequency domain using block-DCT is proposed. The aim of this scheme is to improve the data hiding capacity while maintaining the quality of the stego image. We use block-DCT to transform the cover image into the frequency domain. The block-DCT gives extra security to the secret image as the embedding is done on the DCT transformed coefficients of the cover image and not directly onto the pixels of the cover image as is done with data hiding in the spatial domain. In the frequency domain we quantize the cover image before the embedding process is carried out. The proposed scheme uses base notation to perform the data hiding. This scheme improves the quality of stego image, the data hiding capacity and also, the secret image is completely reconstructed.**

Index terms –Data Hiding, steganography, frequency domain, block-DCT, information and data security.

I. INTRODUCTION

In the networking world, technology is growing exponentially. But with this improvement in technology there is a large threat to the information being transferred. With every counter measure taken against attacks to the security of information there is always a counter attack found. These days there is a huge need for data protection. This data may be flowing through a network and may be in various forms, textual, images, videos, etc. At any time some information may fall into the wrong hands. There are various encryption algorithms used these days to convert information into meaningless data inorder to protect it. Some of the famous encryption schemes are, RSA [1] and DES [2]. In this paper we concentrate on a particular type of technique called data hiding. Data hiding is also referred to as steganography sometimes.

Steganography can be referred to as a technique in which information is hidden so as to prevent the detection of hidden messages [3, 4]. There are many methods to perform this hiding. Few methods of data hiding that have been employed are invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications [5]. A conventional technique for data hiding is performed by hiding information onto a single host image that we will here refer to as the cover image. The image that we get after information is hidden in the cover image is called the stego image. Data hiding can be done on the cover image in the spatial domain or the frequency domain. Data hiding in the spatial domain may be done by directly hiding the data into the pixels of the cover image. Fig. 1 shows the basic data hiding process. Techniques like least significant bit (LSB) substitution may be used for the hiding process. For data hiding in the frequency domain we can use the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT) to transform the images into the frequency domain [4, 6].

In this paper we concentrate on data hiding in the frequency domain. Here, we use DCT to transform the image into the

Fig. 1 Basic data hiding process

frequency domain. The advantage of performing data hiding in the frequency domain instead of in the spatial domain is that the hiding is done on the transformed coefficients and not directly onto the pixels of the cover image. Since the hiding is done on the coefficients of the transformed image the security of the secret image is higher.

There are many techniques that have been previously proposed when it comes to data hiding in the frequency domain. Most of them are data hiding schemes developed for DCT-based compressed images. In the proposed scheme we aim to improve the data hiding capacity, quality of reconstructed secret image of previous schemes. The description of other related schemes are given in the following section.

The following sections of the paper is organized as follows. Section 2 explains some related works in the field of data hiding. Section 3 describes the proposed scheme. The experimental results and analysis are shown in Section 4. Section 5 gives the conclusion of this paper.

II. RELATED WORK

In this section we review the various concepts required to understand the proposed scheme. We also briefly discuss the previously proposed data hiding techniques in the frequency domain.

A. *Discrete Cosine Transform (DCT)*

Discrete Cosine Transform is used to transform an image into the frequency domain. It removes the sine component of the image. This is generally used for image transformation and compression [7].

The mathematical definition of 2-dimensional DCT performed on an 8 × 8 block is given in Eq. (1). In the equation $F(u, v)$ is the DCT of $f(x, y)$.

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

$$\text{where } C(e) = \begin{cases}\frac{1}{\sqrt{2}}, & if\ e = 0\\ 1, & if\ e \neq 0\end{cases}$$

The mathematical definition of 2-dimensional inverse DCT performed on an 8 × 8 block of pixels is given in Eq. (2).

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

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig. 2 The standard quantization table

B. *Quantization*

Quantization is used in image processing for lossy compression. It is done by compressing a continuous range of values to a discrete range of values [7]. The property exploited in this compression technique is if the number of discrete pixels in block of image is reduced then the image becomes compressible. This is done by dividing each coefficient of a block in the DCT transformed cover image by integers in a quantization table. The standard quantization table used for this purpose is given in Fig. 2.

C. *Chang et al.'s data hiding scheme*

Chang et al.'s [8] scheme embeds the secret bits into the DCT-based compressed image. This is a reversible scheme hence the original coefficients can be restored after secret bits have been extracted. In this scheme the secret data is embedded into the successive zero sequence in the middle-frequency components. Fig. 3 shows the region that is considered for embedding.

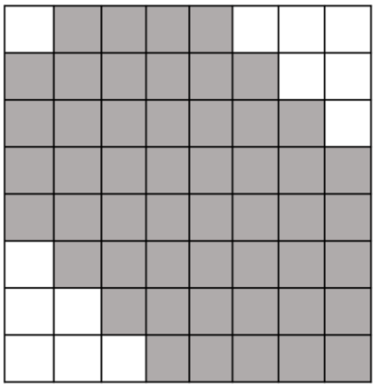

Fig. 3 Coefficients where secret can be embedded

A disadvantage of this scheme is that though it is reversible the data hiding capacity is very low.

D. *Lin et al.'s reversible data hiding scheme*

Lin and Shiu [9] proposed a 2-layer data hiding scheme which is an extension of Chang et al.'s [8] sceheme. Layer-1 is the data hiding strategy proposed here by Lin and Shiu and layer-2 is the one proposed by Chang et al. Tian's pixel expansion method [10] is used to design layer-1. Layer-1 is used to consider some areas that were not used by Chang et al.'s scheme. The reversibility and security of the Chang et al.'s scheme is maintained in this scheme.

III. PROPOSED SCHEME

The previous schemes have very low data hiding capacity as they hide data only by making modifications depending on the successive zero coefficients of the DCT transformed cover image. This limits the secret to be embedded only to parts of the 8 × 8 block of a cover image. The main objective of the other schemes is to compress the cover image and maintain the reversibility. In this paper the quality of the stego images nad the reconstructed secret images are the main concern. The previous schemes offered reversibility of the stego images at the cost of low data hiding capacity. We now explain in detail the various phases in the proposed scheme.

A. *The Pre-processing Phase*

The pre-processing phase is the phase in which the cover image is prepared for data hiding phase. The following steps describe the processes the cover image undergoes:

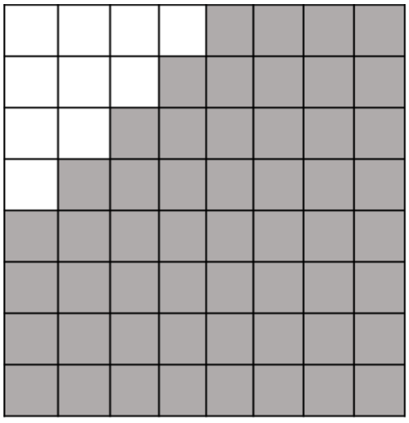

Fig. 4 Coefficients where secret can be embedded for our scheme

1) *8 × 8 Block Preparation and Block-DCT:* The Cover image is divided into non-overlapping blocks of size 8 × 8 pixels each. Then each block is transformed into the frequency domain by using the formula given in Eq. (1).

2) *Quantization:* The DCT transformed cover image now undergoes quantization. Generally the reason for quantization

3) *8 × 8 Block Preparation and Block-DCT:* The Cover image is divided into non-overlapping blocks of size 8 × 8 pixels eis to achieve compression. In the proposed scheme, the reason for using quantization is that since DCT coefficients are floating point numbers it is not possible to perform integer arithmetic on them. So we need to quantize all the pixels of the image. Chang et al. [8] and Lin et al. [9] have used the standard quantization table that will just satisfy our purpose of getting a stego image with good quality. In the quantization phase we divide each of the DCT coefficients by the corresponding number in the quantization table.

B. *The Data Hiding Phase*

The secret data will not be hidden in the entire 8 × 8 blocks but just a part of it. We tried embedding information into various sections of a block and we came up with the best area to embed the information. The area in which the information is being embedded is given in Fig. 4. We now describe the steps involved during the data hiding phase.

1) *Preparing the Secret image:* Convert all the pixels in the secret image into a base-8 system. Let one pixel be represented by S. For example, $S = (62)_{10} = (76)_8$.

2) *Prepare pixels of cover image:* Two adjacent pixels of the cover image are taken and transformed into one integer as in Eq. (3).

$$I = A \times 3^0 + B \times 3^1 \ (mod\ 8) \qquad (3)$$

For example, suppose 1 and 2 are two adjacent pixels, then the integer can be written as: $I = 1 \times 3^0 + 2 \times 3^1 \ (mod\ 8) = 7$.

3) *Combine the Secret pixel and the pixel from the cover:* This is done using the following expression in Eq. (4).

$$s = S(i) - I + 4 \ (mod\ 8) \qquad (4)$$

where, S is a secret pixel in base-8 system and i denotes the position of the value. For example, in $S = (76)_8$ we have, $S(1) = 0$, $S(2)=7$ and $S(3) = 6$. Therefore, for $S(1) =7$, $s = 7\text{-}7\text{+}4 \pmod 8 = 4$.

4) *Transform s into a base-3 notation:* The reason why we chose to convert the pixels in the secret to base-8 notation is understood in this step. As, 7 is the largest number that can be transformed into a base-3 notation and still be of length 2 we use base-3 notation. We can represent *s* in base-3 notation as (s_1, s_2). For example, suppose *s* = 4 then we have *s* base-3 as (1, 1).

5) *Switch the elements of s:* This is done after observing the values during the extraction phase. On switching the elements become (s_2, s_1). In the above example we have *s*= (1,1).

6) *Reduce the value of each element by 1:* This is done so that the modification made to the coefficients of the cover image will be comparatively small. So, $s_2 = s_2$-1 and $s_1 = s_1$-1. In the example we have *s* = (0,0).

7) *Modify the coefficients of the cover image:* This is done using the expressions given in Eq. (5).

$$A' = A + s_2 \; and \; B' = B + s_1 \qquad (5)$$

For the example above we have A' = 1+0 = 1 and B' = 2+0 = 2.

8) *Obtain the stego image:* We follow steps 1 through 7 until all the pixels of the secret image has been embedded into the cover image. The stego image is now obtained by performing de-quantization followed by IDCT on this modified cover image. IDCT is performed by carrying out the operation given in Eq. (2).

C. The Data Extraction Phase

In the receiver side we have the stego image from which the secret image has to be extracted. The stego image is first undergoes pre-processing as given in section A above. After this, the stego image undergoes the following steps:

1) *Prepare pixels of stego image:* Two adjacent pixels of the stego image are taken. Let them be, $A'$and B'. For example, A'= 1and B'= 2.

2) *Extract the i^{th} integer value from $A'$and B':* This is done by using the expression given in Eq. (6).

$$S(i) = A' \times 3^0 + B' \times 3^1 \; (mod\ 8) \qquad (6)$$

For example, $S(i)$=1 × 3^0 + 2 × 3^1(mod 8) = 7.

3) *Obtain the secret pixel:* Step 2 is repeated till we get the entire pixel value S. Now S is converted to base-10 notation from base-8 notation. For example, $S = (076)_8 = (62)_{10}$.

4) *Obtain entire secret image:* Step 1 through Step 3 is repeated till the entire secret image is obtained.

IV. Experiments and Results

In this section we give results of some of the experiments carried out to evaluate our scheme. We implement this scheme using grayscale images. We need to compare this scheme with respect to previous schemes. For evaluating this scheme we measure the Peak Signal to Noise Ratio (PSNR) values as given in Eq. (7).

$$\text{PSNR} = 10 \times log\left(\frac{255^2}{\text{MSE}}\right) \qquad (7)$$

MSE is also known as Mean Square Error. The MSE for an image of size $M \times N$ can be calculated as follows,

$$\text{MSE} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\frac{(f(x,y) - g(x,y))^2}{M - N} \qquad (8)$$

TABLE I
PSNR and Capacity Comparison Of Stego Image

Cover Images	PSNR (dB)					
	Chang et al's scheme [9] L=9		Lin and Shiu's Scheme [10]		Proposed Scheme	
	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity
Boats	27.49	36817	31.95	58357	44.83	110592
Airplane	27.73	36852	33.21	57889	44.94	110592
Lena	28.13	36861	34.01	57644	44.86	110592
Baboon	24.22	36094	26.75	66048	44.79	110592
Peppers	28.54	36842	34.10	56936	44.83	110592
Zelda	29.5	36864	35.28	55184	44.90	110592

where, $f(x, y)$ is the original pixel value of the cover and $g(x, y)$ is the pixel value of the stego image at the coordinates (x, y). The PSNR is most commonly expressed in dB. The higher the PSNR value the better the quality of the stego image as the noise in the image is less. A PSNR value with less than 30 dB is considered to be poor as a lot of significant information has been lost.

We also calculate the hiding capacity of this scheme. By hiding capacity we mean the number of pixels of the secret that can be hidden in a cover image. In Table I we compare the PSNR and the hiding capacity between the previous schemes and the proposed scheme.

By observing the PSNR values in Table I it is clear that the proposed scheme gives much higher quality stego images than the previous schemes. There is an increase of over 10 dB in the PSNR values due to mainly the use of the customized quantization table. Also, we have an increase in the hiding capacity of the cover images. This is basically due to the fact that a different embedding area is used as compared to the previous schemes. During experiments it is also observed that the secret value can generally be completely reconstructed. As mentioned previously in this scheme we are not interested in the compression factor but on the quality of the stego images, the hiding capacity and the quality of the secret images. Experiments show that all those criteria are satisfactory.

V. CONCLUSIONS

In the proposed scheme we have used DCT as it is the most widely used mechanism for frequency transformation. Also, the security of the secret pixels are maintained. The previous schemes dealt with DCT-based compressed images. In our scheme we have improved the stego image quality as well as the capacity of the cover image.

The previous schemes maintained reversibility of the cover images at the cost of the capacity. Reversibility of a stego image ensures that once the secret image from the stego image is extracted then we can get back the cover image. Our scheme does not offer the reversibility function. Our future work would be to include the reversibility function in this scheme.

REFERENCES

[1]. R. L. Rivest, A. Shamir and L. Adelman, A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, col. 21, no. 2, pp. 120-126, Feb. 1978.

[2]. W. Diffie and M. E. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, IEEE computers, vol. 10, pp. 74-84, 1977.

[3]. L. Bai, S. Biswas and P. E. Blasch, "*An Estimation Approach to Extract Multimedia Information in Distributed Steganographyic Images*," in Proc. 10th International Conference on Information Fusion, Quebec, Canada, 2007.

[4]. F. N. Johnson, S. Jajodia, Exploring Steganography: Seeing the Unseen, Proceedings IEEE paper of February, 1998.

[5]. A. Cheddad, J. Condell, K. Curran, M. P. Kevitt, "*Digital Image Steganography: Survey and Analysis of Current Methods*", Proceedings of ELSEVIER Journal on Signal Processing 90, 2010, 727-752.

[6]. B. Ki, J. He, J. Huang, Y. Q. Shi, A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, 2011.

[7]. R. C. Gonzalez, R. E. Woods, *Digital Image Processing*, 3rd ed., Pearson Education, 2011.

[8]. C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, Reversible hiding in DCT-based compressed images, *Information Sciences*, vol. 141, 2002, pp. 123-138

[9]. C. C. Lin and P. F. Shiu, DCT-based reversible data hiding scheme, Proc. Of the 3rd International Conference on Ubiqutous Information Management and Communication (ICUIMC'09), pp. 327-335, 2009.

[10]. J. Tian, "Reversible data embedding using a difference expansion", IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug. 2003