A Novel Steganographic Technique Based on 3D-DCT Approach

Samir Kumar Bandyopadhyay
Department of Computer Science and Engineering, University of Calcutta
Kolkata-700009, India
E-mail: skb1@vsnl.com

Tuhin Utsab Paul
Department of Computer Science and Engineering, University of Calcutta
Kolkata-700009, India
E-mail: tuhin@ieee.org

Avishek Raychoudhury
Department of Computer Science and Engineering, University of Calcutta
Kolkata-700009, India
E-mail: avishekraychoudhury@gmail.com

Abstract

In this paper, a new technique for hiding the data of images has been proposed. This method uses 3-dimentional discrete cosine transformation scheme, along with 2-dimentional discrete cosine transformation. The method proposed in this paper hides two target images behind one cover image thereby increasing the data hiding capacity greatly. For the cause of security only the final stego-image is sent over the network. This approach is also free from the constraint of size.

Keywords: Data, image, Hiding, Security, Encryption, Discrete cosine transformation

1. Introduction

Steganography, coming from the Greek words *stegos*, meaning roof or covered and *graphia* which means writing, is the art and science of hiding the fact that communication is taking place. Steganography is the art of hiding, and transmitting information using apparently innocent carrier without expose any suspicion. Generally, in steganography the following operations are performed:

1) Write a non-secret cover message.

2) Produce a stego-message by concealing a secret embedded message on the cover-message by using a stego-key.

3) Send the stego-message over the insecure channel to the receiver.

4) At the other end, on receiving the stego-message, the intended receiver extracts the secret embedded message from the stego-message by using a pre agreed stego-key.

Figure 1: Block diagram of steganography

Steganography using 3-dimentional discrete cosine transformation aims on hiding images(s) behind another image. This proposed method transforms a block of integrated composite image i.e,coverimage + targetimage1 + targetimage2 into the frequency domain using 3-dimentional discrete cosine transformation. The proposed algorithm transmits a reddish image (stego-image) from the sender end which is the result of 3-D DCT and subsequent 2-D IDCT on the composite image (coverimage + targetimage1 + targetimage2). On the receiver end, the individual cover image, targetimage1 and targetimage2 are recovered by using 3-D Inverse discrete cosine transformation and 2-D DCT.

To the best of our knowledge, this concept of 3-D DCT is wholly a new concept of converting a cube of spatial domain values to the frequency domain value. The reverse is done using 3-D IDCT. This concept is based on the concept of 2-D DCT.

Lastly, the main advantage of this proposed method is that two images can be hidden behind one image. Moreover during transmission, a complete new image (different from cover or target images) is transmitted over

network thereby reducing the chance of suspicion of the network eavesdropper.

2. Related works

The majority of today's steganographic systems uses images as cover media because people often transmit digital pictures over email and other Internet communication. Several methods exist to employ the concept of Steganography as well as plenty algorithms have been proposed in this regard. To gather knowledge regarding our approach, we have concentrated on some techniques and methods which are described below.

In the field of image security, Miroslav Dobsicek (Dobsicek, M., 2004) has developed an interesting application of steganography where the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information. Yusuk Lim, Changsheng Xu and David Dagan Feng, 2001, described the webbased authentication system consists of two parts: one is a watermark embedding system and the other is authentication system. In case of watermark embedding system, it is installed in the server as application software that any authorized user, who has access to server, can generate watermarked image. The distribution can use any kind of network transmission such as FTP, email etc. Once image is distributed to externally, client can access to authentication web page to get verification of image (Yusuk Lim, Changsheng Xu and David Dagan Feng, 2001).

Min Wu and Bede Liu, June, 2003, proposed (Min Wu. 2004) a new method to embed data in binary images, including scanned text, figures, and signatures. The method manipulates "flippable" pixels to enforce specific block based relationship in order to embed a significant amount of data without causing noticeable artifacts. They have applied Shuffling before embedding to equalize the uneven embedding capacity from region to region. The hidden data can then be extracted without using the original image, and can also be accurately extracted after high quality printing and scanning with the help of a few registration marks.

Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al- Taani, 2005, have explained a method with three main steps. First, the edge of the image is detected using Sobel mask filters. Second, the least significant bit LSB of each pixel is used.

Finally, a gray level connectivity is applied using a fuzzy approach and the ASCII code is used for information hiding. The prior bit of the LSB represents the edged image after gray level connectivity, and the remaining six bits represent the original image with very little difference in contrast. The given method embeds three images in one image and includes, as a special case of data embedding, information hiding, identifying and authenticating text embedded within the digital images (Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, 2005). In 2007, Nameer N. EL-Emam proposed an algorithmic approach to obtain data security using LSB insertion steganographic method. In this approach, high security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too(Nameer N. EL-Emam, 2007).

S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das in 2008 has proposed a heuristic approach to hide huge amount of data using LSB steganography technique. In their method, they have first encoded the data and afterwards the encoded data is hidden behind a cover image by modifying the least significant bits of each pixel of the cover image. The resultant stego-image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique (S.K.Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das, 2008).

There is also a good method proposed by G. Sahoo and R. K. Tiwari in 2008. Their proposed method works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography. And due to this reason they have used a stego key for the embedding process (G. Sahoo, R. K. Tiwari, 2008).

Unfortunately, modifying the cover image changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego-image's statistical properties. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way. So, in order to obtain more security in our prescribed method, we have embedded an entire image behind another image of twice the size of target image remarkable change in the final image.

3. Our Work

3.1 3-D DCT:

The three-dimensional variant of the DCT is a composition of three 1D DCT along each dimension. The formal definition is:

Figure 2: Formulation of 3D DCT

where $x(i, j, k)$ is a value of the video cube element which is positioned at the coordinates i, j, k , $X(l,m, n)$ is a 3D DCT coefficient at the position l,m,n and indexes take values $l,m,n = 0,1,...,N-1$.

The $C_{li} \cdot C_{mj} \cdot C_{nk}$ multiplication is the 3D DCT base function which can be defined as :

Figure 3: Formulation for the constraints.

A cube of frequency components is the product of the 3D DCT. It contains one DC coefficient $X(0,0,0)$ at zero coordinates, the remaining 11 coefficients are called AC coefficients. The most important elements of the signal are concerned near this DC coefficient.

3.2 Sender Side Approach:

In the sender side, one coverimage (C) and two targetimage (T1 and T2) are selected. All the images are resized in the size of coverimage C using bi-cubic interpolation. All the images are converted into gray scale. Then these three images are integrated as a composite image by placing the coverimage (C) in the first plane, targetimage1 (T1) in the next plane ad targetimage2 (T2) in the last plane. Thus this integrated composite image is a color image different from C,T1,T2. Then 3-D DCT is applied on each 4*4*3 cubical segment of the composite image. Of this block obtained by 3-D DCT, the first four values i.e, of the first plane is taken and 2-D IDCT is performed. The other AC components are quantized. Thus the cube is formed where the first plane has large values and the other planes has low values. This is done until the whole composite image is transformed. Then this is transmitted to the receiver end as the stego image which is different from C,T1,T2 and mostly reddish in texture.

Figure 4: Sender side approach

3.3 Receiver side approach:

In the receiver side a stego image is received. This image is mostly reddish in color. Block of 4*4*3 pixel values is selected. The first four pixels values i.e, of the first plane is taken and 2-D DCT is applied on them. The result is clubbed with the other pixel values of the remaining two layers. The whole cube is then transformed using 3-D IDCT. This is continued until the whole stego image is transformed. The target image T1 is retrieved from the second layer and T2 from the third layer of the transformed stego image.

Figure 5: Receiver side approach

3.4 Algorithms:

The formal algorithms are as follows:

3.4.1 Sender end:

This module will be used in the sender side.

Input: This function will take Target Image1, Target Image2 and Cover Image as input.All the input images must be grayscale image.

Output: It will output the encoded stego-image.

1) Read the the Cover Image and 2 target images Target Image1, Target Image2.

2) Resize the 3 images using bi-cubic interpolation to a equal size where both the rows and columns are even.

3) Create two 3-d matrix A of whose each plane is of the size of the resized images and B of size (2X2X3).

4) Store the pixel values of 3 images in the 1^{st},2^{nd} and 3^{rd} plane of 'A' respectively.

5) Store the adjacent quadruple values of the 3 planes of A and store it in the corresponding planes of B.

6) Calculate the 3-D DCT of B and store it in B. Then calculate the 2-D IDCT of the 1^{st} plane of B and store it in the 1^{st} plane of B.

7) Store the values of 1^{st},2^{nd} and 3^{rd} plane of 'B' in the corresponding quadrant of 1^{st},2^{nd} and 3^{rd} plane of 'A' respectively.

8) Move to the next quadrant of 'A' until 'A' is exhausted and repeat step 5 to step 7.

9) Return the new matrix 'A' as Stego-Image.

3.4.2 Receiver end:

This function will be used in the receiver side.

Input :: This function will take Stego-Image as input.

Output :: It will output the decoded 2 Images.

1) Read the Stego-Image and calculate its size.

2) Take two 3-d matrix A whose each plane is of the size of Stego-Image and B of size (2X2X3).Store the 1^{st},2^{nd} and 3^{rd} plane of StegoImage in the corresponding 1^{st},2^{nd} and 3^{rd} plane of matrix A respectively.

3) Store the quadrant values of the 3 planes of A and store it in the corresponding planes of B.

4) Calculate the 2-D DCT of the 1^{st} plane of B and store it in the 1^{st} plane of B.Then calculate the 3-D IDCT of B and store it in B.

5) Store the values of 1^{st},2^{nd} and 3^{rd} plane of 'B' in the corresponding quadrant of 1^{st},2^{nd} and 3^{rd} plane of 'A' respectively.

6) Move to the next quadrant of 'A' until 'A' is exhausted and repeat step 3 to step 5.

7) Take 2 matrix C and D of size of the Stego-Image.Store the 2^{nd} and 3^{rd} plane of A in C and D respectively.

8) Retrieve TargetImage1 and TargetImage2 from 2 matrices C and D respectively.

4. Computation Complexity:

At the sender side, the 3D-DCT has a computational upper bound of $O(n^3)$ and the 2-D IDCT has a computational complexity of $O(n^2)$. The two processes are performed in serial. So the total computational complexity of the sender side algorithm is $O(n^3)$.

At the reciever side, the 3D-IDCT has a computational upper bound of $O(n^3)$ and the 2-D DCT has a computational complexity of $O(n^2)$. The two processes are performed in serial. So the total computational complexity of the sender side algorithm is $O(n^3)$.

5. Conclusion

The 3D DCT is the most time demanding part of the whole compression process, it should be simplified as possible. The same is true for inverse discrete cosine transformation. The most elegant feature of this proposed algorithm is that it hides two images at a time thereby increasing the data hiding capacity hugely.

The encryption method using the 3D DCT was examined and its progress was described. Similarly the decryption method using the 3D IDCT was examined and its progress was also described. Main tasks which will be necessary to work out and their possible solutions were discussed. The future steps will be deeper research of outlined problems. Because the DSP implementation should be the main task of further work, the investigation will aim this way.

References

Dobsicek, M. (2004). Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization", January 2008, IJCSNS, Vol. 8, No. 1,Page(s): 228 – 2336.

Min Wu. (2004). Member, IEEE, and Bede Liu, Fellow, IEEE, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004 Page(s): 528 - 538

Nameer N. EL-Emam. (2007). "Hiding a large amount of data with high security using steganography algorithm", *Journal of Computer Science.* April 2007, Page(s): 223 – 232

Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani. (2005). "Data Embedding Based on Better Use of Bits in Image Pixels", *International Journal of Signal Processing* Vol 2, No. 2, 2005, Page(s): 104 - 107

S.K.Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das. (2008). "A Secure Scheme for Image Transformation", August 2008, IEEE SNPD, Page(s): 490 – 493

S.K.Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das, "A Secure technique for Image data hiding".

Yusuk Lim, Changsheng Xu and David Dagan Feng. (2001). "Web based Image Authentication Using Invisible Fragile Watermark", 2001, *Pan-Sydney Area Workshop on Visual Information Processing* (VIP2001), Sydney, Australia, Page(s): 31 - 34

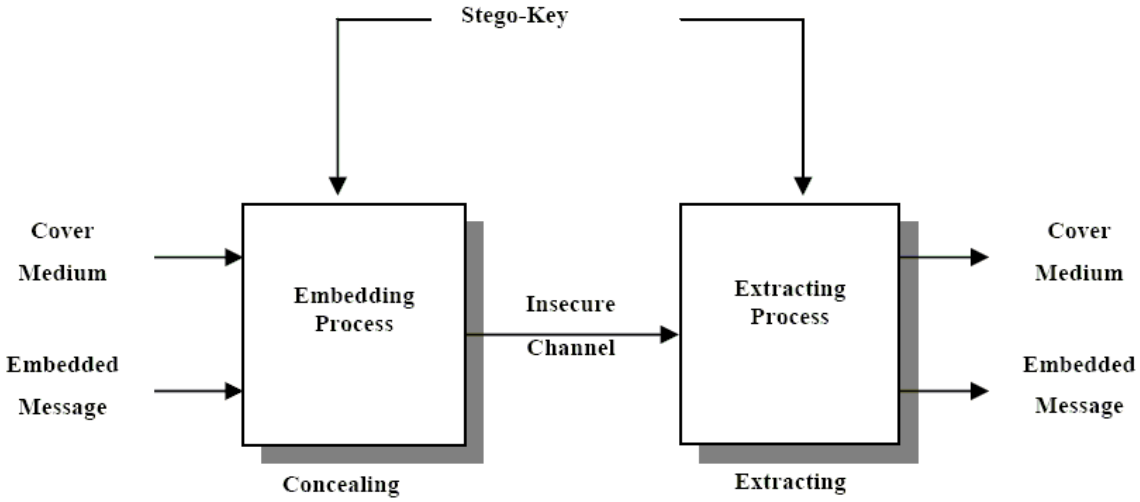

Fig. 1: The General Steganography System

Figure 1. Block diagram of steganography

The above figure shows the basic blocks of steganography consisting of two basic operations, concealing and extracting.

$$X(l,m,n) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\sum_{k=0}^{N-1} x(i,j,k)\cdot C_{li}\cdot C_{mj}\cdot C_{nk}\ ,$$

Figure 2. Formulation of 3D DCT

The above figure shows the mathematical equation for 3-dimentional Discrete Cosine Transformation.

$$C_{li}\cdot C_{mj}\cdot C_{nk} = \cos\left[\frac{\pi}{N}\left(i+\frac{1}{2}\right)l\right]\cdot\cos\left[\frac{\pi}{N}\left(j+\frac{1}{2}\right)m\right]\cdot\cos\left[\frac{\pi}{N}\left(k+\frac{1}{2}\right)n\right].$$

Figure 3. Formulation for the constraints

The above figure shows the formulation of mathematical constrains of the equation of 3-dimentional Discrete Cosine Transformation.

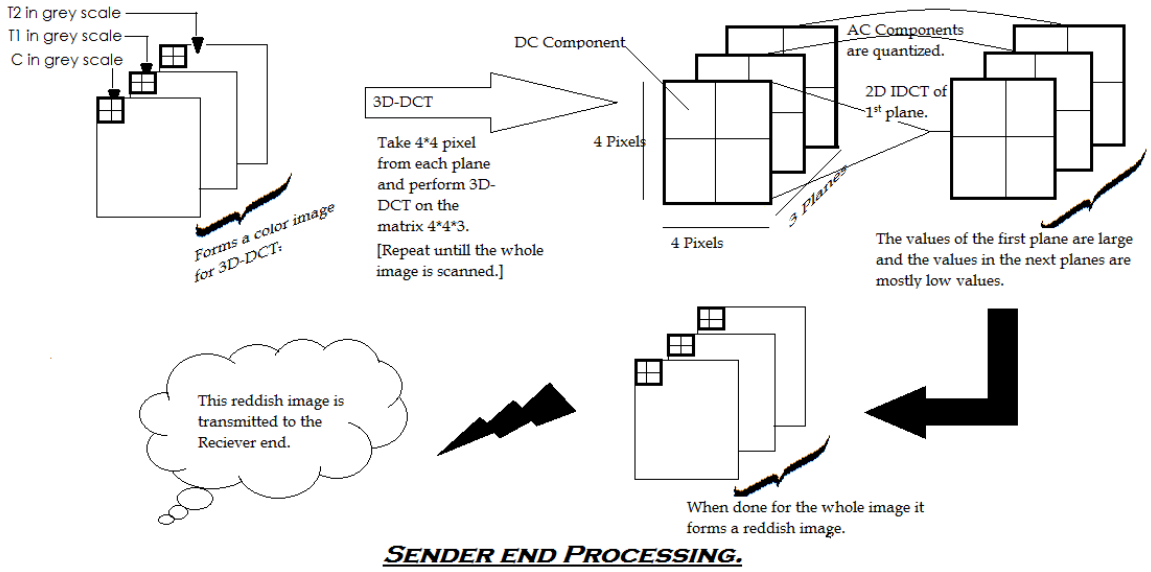

Figure 4. Sender side approach

This figure shows the sequence of proceedings that are to be performed at the sender end.

 ISSN 1913-8989 E-ISSN 1913-8997

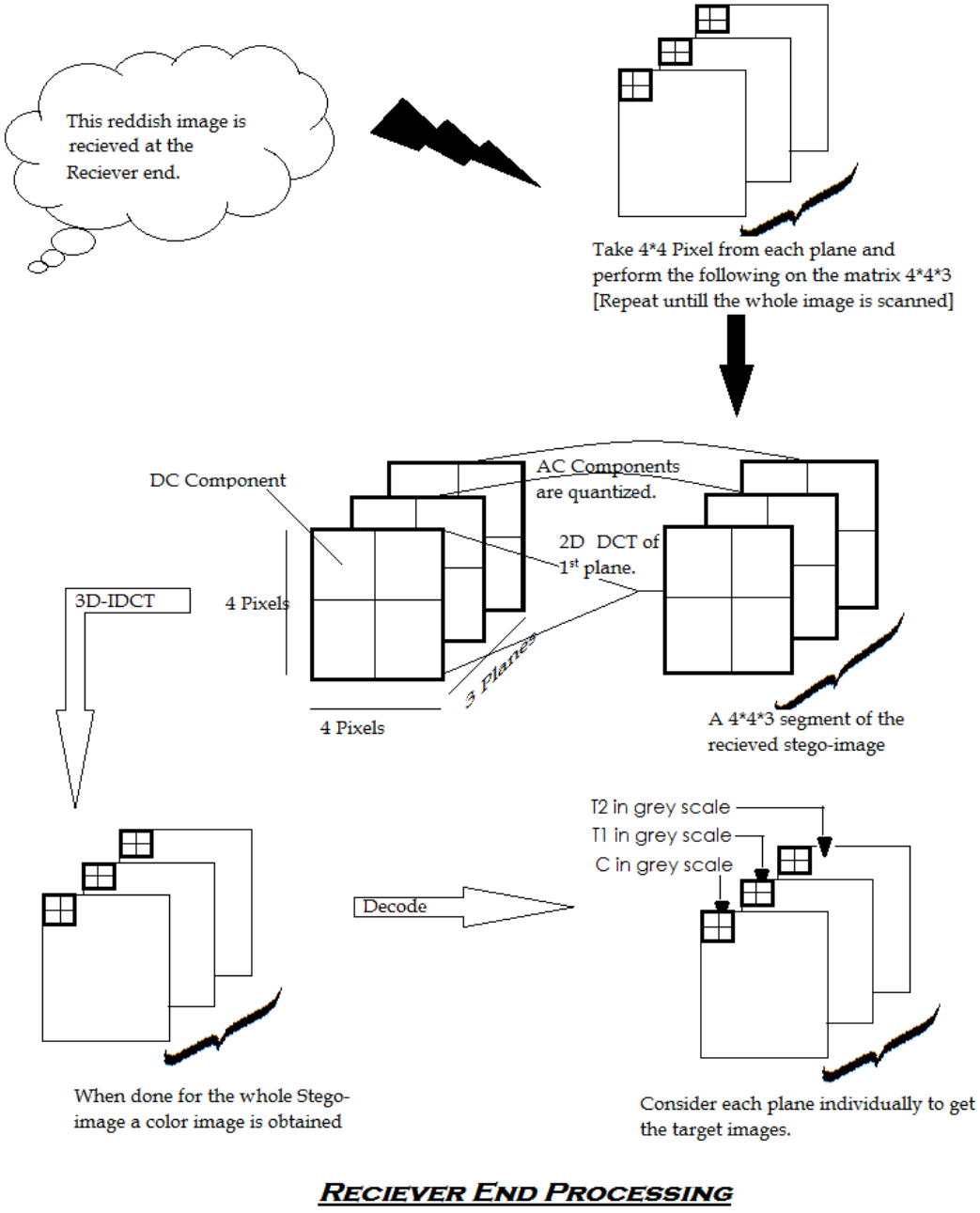

Figure 5. Receiver side approach

This figure shows the sequence of proceedings that are to be performed at the receiver end.