Hiding an Image within another Image using DCT Algorithm

[1]Prof. S. Sabeena, [2]Mr. R. R. Prajith Kumar, [3]Mr. M. Gokul

[1]Assistant Professor, [2,3]Students
Department of Software Systems
Sri Krishna Arts and Science College
Coimbatore, India.

***Abstract*- Due to the lightning development in digital communication through the international networks and all the multimedia works are released via internet, it's an urgent need now to safeguard the data from cruel attacks. So securing data has become an important problem in this field. Image data protection is the essential part in communication and multimedia world. During storing and sharing, avoid third party access of data is the challenging thing. Delivering security of data is the clever work and art also. Multiple protection algorithms are applied in recent times. Data can be safeguarded by transforming the original image into an unfamiliar format, such as signals or sketches, making it incomprehensible to anyone.**

Steganography is the art of hiding information into a cover image. This paper presents a novel stegano graphic method for hiding a secret Image inside the cover image. It exploits the use of host data to hide a piece of information in such a way that it's indistinguishable to human spectator. It's garnering considerable attention these days because it doesn't bring awareness to the presence of its information. The major purposes of effective Steganography are High Embedding Capacity, Imperceptibility and Robustness. The proposed algorithm uses Discrete Cosine Transform (DCT) for cover image. The cover image is segmented into 8 * 8 blocks and DCT is applied on the picture. DCT algorithm is executed in frequency domain in which the cover image is converted from spatial domain to the frequency domain and is segmented into 8 * 8 blocks also the secret image data bits are fitted into the frequency elements of the cover image. It's observed that the proposed algorithm is more robust with better Mean Square Error (MSE), Peak Signal to Noise Rate (PSNR), Character Error Rate (CER) & Normalized coefficient.

***Keywords*: Steganography, DCT, Stego-Image, MSE, PSNR, CER.**

1. INTRODUCTION

Steganography is a approach in which data can be hide into another information, the information like as image, audio, video filesetc. The data can be simple text message, any image files or may be an audio clip. The algorithm employed forhide the information into the information is known as stego algorithm, where as the unauthorized way to extract the information is called stego analysis. Medium integrity poses a significant concern in steganography, where embedding one form of media into another should not compromise the originality of the cover media. The suggested method relies on the manipulation of the least significant bits, which replaces DCT coefficient value of pixels. The fundamental LSB-based technique entails replacing the least significant bit plane of the host image with the bit sequence representing confidential data. These approaches are based on false supposition that LSB plane of natural images is random enough, hence are suitable for data hiding. Such supposition isn't always true, especially for images with further smooth regions.

The DCT of the carrier image is first obtained, and then appropriate threshold random positions are selected. Subsequently, the least significant bits(LSBs) of these selected positions in the carrier image are replaced with the most significant bits (MSBs) of the secret image.Security is provided to an image,by encrypting the image with the help of Key and generates stego image[1]. This secured image is also transmitted to the receiver, this stego image is accepted and the original image is also achieved with the help of Key. In Figure1.1, Steganographic system is explained with simple block illustration (ie) secret image will be hided inside the cover image and stego image is processed[2].

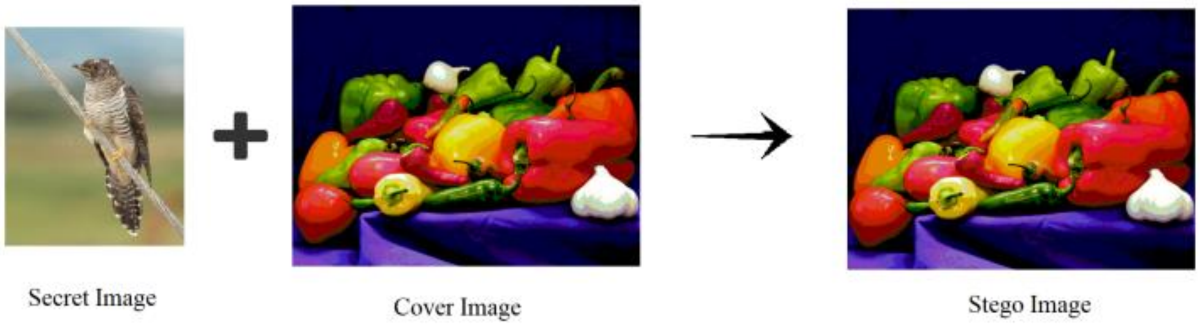


Figure 1.1 Simple Block Diagram of Steganographic System

1.1 Overview of Steganography

The secret message generally is a text document or another image file which contains the secret information. This information is transferred to the encoder unit in the first step. The encoder must be designed and enforced with high accuracy, to hide the secret message with a limited deformation and changes in the cover image. Encoder unit generally needs a key to increase the security degree of hiding technique; Without using this key, the message will be available without any interference, if someone guesses the embedding or extraction algorithm. The output of the encoder unit, referred to as the steganogram, should closely conceal the data. Additionally, both this image and the key utilized during the embedding phase are transmitted through a communication channel. In the succeeding step this package are applied to decoder unit. Result of the decoder unit is delivered in the receiver side. The result of extracted unit is just an estimate of secret message, because during transmission through the communication channel, the steganograme is exposed to different types of noises, which can change the values of some bits. The usage of steganographic approach can be highly classified as operating in two different phases, such as spatial phase and frequency phase. In spatial domain, the embedding and concealment process are mostly carried out by bitwise manipulation. For instance,

Altering the least significant bit (LSB) within one of the color channels in an image, whereas in the frequency domain, methods involve manipulating transformed images such as Discrete Cosine Transformation (DCT) and wavelet transformation. Similar manipulation includes changing the value of the quantized DCT coefficients.

2. Discrete Cosine Transform

In Discrete Cosine Transform, for each color element. The JPEG image format employs a discrete cosine transform.to transform sequential 8 x 8 pixel blocks of the image into 64 DCT coefficients each. The Discrete Cosine Transform (DCT) coefficients F(u, v) for an 8 x 8 block of image pixels f(x, y) are defined as follows:

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

Where,

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, if\ u \leq 0 \\ 1, if\ u > 0 \end{cases} \quad [5]$$

The algorithm to embed the image is shown in Figure 2.1 and is as follows

Step 1: Read cover image.
Step 2: Retrieve the secret image and convert it into binary format.
Step 3: The cover image is divided into 8 × 8 blocks of pixels.
Step 4: Starting from the top-left corner and moving left to right, then top to bottom, subtract 128 from each pixel value within each block.
Step 5: The DCT is performed on every block
Step 6: Each block is compressed
through quantization table.
Step 7: Calculate LSB of DC
coefficient and replace with each bit of the secret image.
Step 8: Generate the stego image

Figure 2.1 Flowchart of Embedding Algorithm

The procedure for recovery using the DCT approach is illustrated in Figure 2.2.

Step 1: Retrieve the stego image.
Step 2: Divide the stego image into 8 × 8 blocks of pixels.
Step 3: Iterating from left to right and top to bottom, subtract 128 from each block of pixels.
Step 4: Apply DCT processing to each block.
Step 5: Compression of each block occurs using a quantization table.
Step 6: Determine the least significant bit of each DC coefficient.
Step7: Recover and convert each 8 bits into a character.

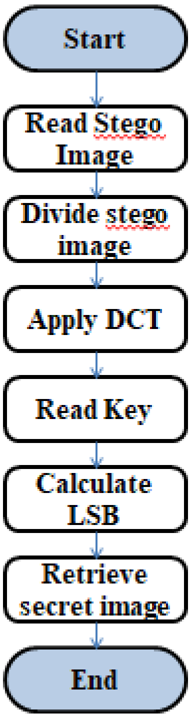


Figure 2.2 Flowchart of Extracting Algorithm

The DCT block F consists of 64 DCT coefficients. The top left portions F (0,0) correlates to lower frequency of the original image block, which is called DC coefficient. As we move down from the F (0,0) in all directions the DCT coefficients correlate to higher and higher frequencies, where F (7,7) corresponds to the highest frequency.[9]
An example DCT block is depicted in Table 2.

Table 2 DCT Block

162	40	20	72	30	2	-1	-1
30	108	10	32	27	5	8	-2
-94	-60	12	-43	-31	6	-3	7
-38	-83	-5	-1	4	-6	1	-6
-31	17	-5	-1	4	-6	1	-6
0	-1	2	0	2	2	8	2
4	-2	2	6	8	-1	7	2
-1	1	7	6	2	0	5	0

A useful point in the JPEG process in this step varying image contraction and quality is accessible through the selection of specific quantization table. The standard quantization matrix JPEG uses quality factor (α) 50 that as shown in Table.2.1. In another degree of quality and contraction asked, scalar multiples of the JPEG standard quantization matrix may be used. The measured quantization matrix is then rounded and trimmed to have positive integer values ranging from 1 to 255. For a quantity position greater than 50, lower contraction and high image quality are attained. For a quantity position lower than 50, further contraction and low image quality are attained.

Table2.2 Quantization Table

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

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. The quantized DCT portions F^Q (u, v) is calculated by

$$F^Q(u,v) = \left[\frac{F(u,v)}{Q(u,v)}\right]$$

Where Q (u, v) is a 64- element quantization table. The quantized DCT block and dequantized DCT block of Table.2 is shown in Table.2.2 and Table.2.3 respectively.

Table1.2 Quantized DCT Block

16	11	10	16	24	40	51	61
10	4	2	5	1	0	0	0
3	9	1	2	1	0	0	0
-7	-5	1	-2	-1	0	0	0
-3	-5	0	-1	0	0	0	0
-2	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Table2.3 Dequantized DCT Block

160	44	20	80	24	0	0	0
36	108	14	38	26	0	0	0
-98	-65	16	-48	-40	0	0	0
-42	-85	0	-29	0	0	0	0
-36	22	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

The LSB, DCT and contraction approaches are used to enhance the security of the payload and it's noted that secure images with low Mean Squared Error (MSE) and Bit Error Rate (BER) are transmitted without the need for any password.[10].

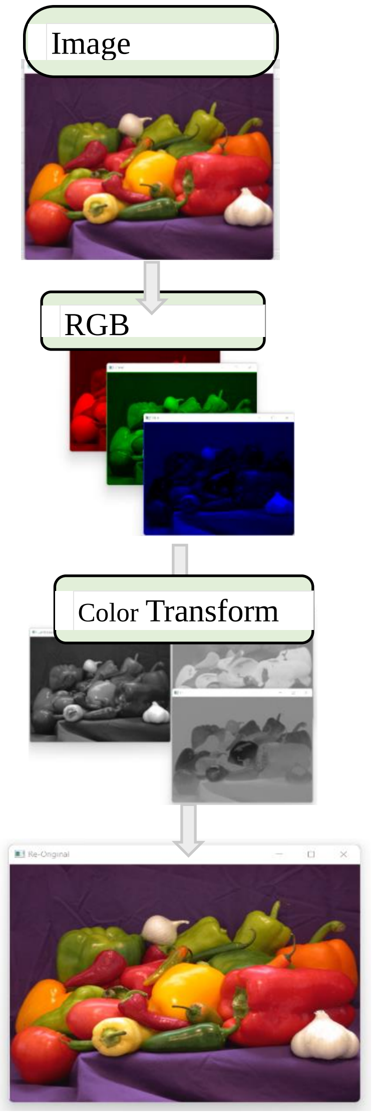
The Double DCT is illustrated wherein all coefficients are binary, and all multiplications are substituted with shifting and addition operations. To save space, downsample the chrominance components of the image. Integer DCT and Affine Transformations ensures the stage image to be visually and statistically undetectable indeed with large payloads. An authentication approach for gray images using DCT, in which the embedding algorithm utilizes DCT on a sub-image block referred to as a mask, with a size of 2 x 2, consisting of spatial components arranged in row-major order across the entire carrier image.

3. Implementation and results:

Cover image is converted into RGB images. By using RGB to YCbCr method RGB images are converted into YCbCr images. Secret image will be converted into stream of bits. These components are incorporated within the Chrominance section of the Cover image. Then the YCbCr will be converted into RGB format. Resultant image will be the stego image[6]. This will send to the receiver. At the receiver end, above process will be followed in reverse order.

This method subtly adjusts the coefficients of the cosine waves employed in reconstructing a JPEG image [3].It works by calculating the frequencies of the each cosine waves in image pixel and then replacing some of them. DCT algorithms are more subtle in the way they manipulate The fast fourier transform that computes the Discrete fourier transform of sequence or its inverse. Fourier analysis transforms a signal from its original domain into a different representation. Photos become much more challenging to detect.

DCT, much like the Fast Fourier Transform (FFT), efficiently approximates lines with a reduced number of coefficients.



JPEG Compression is based on two fundamental assumptions: Grayscale intensity disparities are far more significant than disparities in color. High frequency (rapid and repeated) changes in intensity/color is not visible. Convert image from RGB to YCbCr.Y = Luminance, “Intensity”Cb = Chroma Blue,Cr = Chroma Red[7].

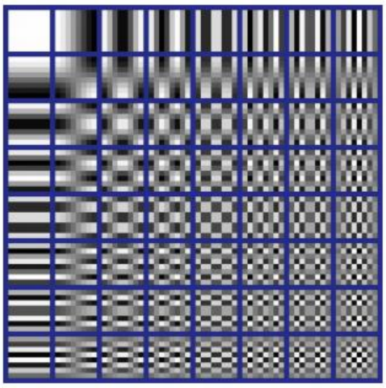


Figure 3.2 8 x 8 DCT

To save space, reduce the resolution of the chrominance components in the image. Normally downsample is by a factor of 4.Most people won’t be able to see too much of a difference.

Typically, a sequence of data points is depicted as the combination of weighted cosine waves. A set of n data points can be depicted by n cosine waves, each with varying frequencies. Splita JFIF image into pixels and apply DCT separately for each pixel. Having 64 data points, each pixel can represent with 64 weighted cosine waves.

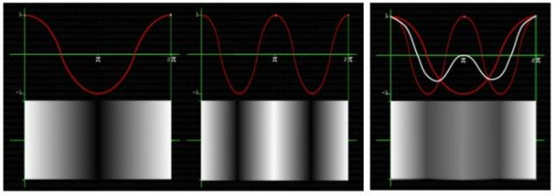


Figure 3.3Cosine waves of various frequencies

In general, A sequence of data points can be expressed as the sum of weighted cosine waves, with each of the n data points being represented by cosine waves of varying frequencies.

REFERENCES:

[1]Blossom Kauret. al. ‘Steganographic Approach For Hiding Image In Dct Domain’Get the idea of using dct algorithm to implement the problem. Published -2011

[2]Kaladharan N Encryption and decryption attain by single key is the previous finest technique of image security. Single key assigned for image encryption and it is encoded. Subsequently the key is safely received and apply decryption process and obtain original image. Published-2014

[3]Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn did Information survey,In which different information hiding techniques are mentioned, like covert channel, anonoymity, stegnography, and copy right making. Published-July 1999.

[4]NielsProvosand Peter Honeyman University of Michigan have mention two different ways of hiding data in to cover image, in sequential method the data is hided in sequential manner by replacing least significant bits of cover image also the F5 algorithm.

F5 uses subtraction and matrix encoding to embed data into the discrete cosine transform (DCT) coefficients. Published- Jun 1, 2003

[5]PrajaktaSuneet. al.

‘Data Hiding in Digital Image Using Steganography’Extracted the LSB technique to encode the text in image.

This technique changes the last few bits in a byte to encode a message, which is especially useful in something like an image. Published- 2007.

[6]Petitcolas FA, Anderson RJ and Kuhn MG, "Information hiding— a survey", Proceedings of IEEE, vol. 87.

[7]N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen", Computer, *vol. 31*

[8]Deepesh Rawat and Vijaya Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, *vol. 64*

[9]M. Preetha et al., "A study and performance analysis of RSA algorithm", International Journal of Computer Science and Mobile Computing, *vol. 2*

[10]Vijay Kumar Sharma and Vishal shrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection", Journal of Theoretical and Applied Information Technology, *vol. 36*