Final Review Document

Image Steganography using Discrete Cosine Transform

Rohan Allen
18BCI0247
9843689966
rohan.allen2018
@vitstudent.ac.in

Ayush Rana
18BCE2305 9003761495
ayush.rana2018
@vitstudent.ac.in

Rakshith Sachdev
18BCI0109
8951822874
rakshith.sachdev2018@vitstudent.ac.in

Rithik Chintala
18BCI0240
9110761940
rithik.chintala2018
@vitstudent.ac.in

Faculty: V. Santhi Ph.D. Head - B. Tech CSE School of Computer Science and Engineering Mobile : 9688138634 Mail Id : vsanthinathan@gmail.com , vsanthi@vit.ac.in

B.Tech. in

Computer Science and Engineering

School of Computer Science & Engineering

Abstract — this paper introduces an algorithm of digital steganography based on Discrete Cosine Transform (DCT). This project aims to convert an image into its frequency domain by use of DCT, and then insert a piece of confidential text that has to be hidden. Steganography and cryptography are used in the proposed process. This method uses DCT steganography and Blowfish encryption algorithm. The encryption algorithm first encrypts the message and DCT steganography hide encrypted message into image. It is widely used and robust method for image compression, it has excellent energy compaction for highly correlated data, which is superior to DFT and LSB. As a result, the majority of functional transform coding systems are based on DCT, which offers a reasonable balance of data packing capability and computational complexity. Also, we capture data loss metrics such as Mean Square Error and Peak Signal to Noise ratio to estimate fidelity and to get a brief idea about the efficiency of the algorithm.

Keywords —Steganography; discrete cosine transform (DCT); discrete wavelet transform (DWT); peak signal to noise ratio (PSNR), mean square error (MSE), high frequency band, streak block.

Introduction:

With the redundancy of the medium as image and voice, digital watermarking technology is to use the digital embedding method to hide the secret information into the digital products of image, visible and video. Seen form the field of signal process, the hidden signal being embedded into carrier is as a feeble signal to add into a strong background. Before going deep into the steganographic process, first and foremost, we need to understand the various components of a steganographic message. The below list covers all the possible components that will be present in the steganographic message. Secret message, Cover data and Stego message. The secret message refers to the part of the message which is intended to be hidden. This message will later be encrypted to make it even more difficult for anyone who tries to break the security to get hold of the hidden informatic message. This is the crucial component in a steganographic message. Next part is the cover data component. This component refers to the container in which the secret message is hidden. This cover data component can be anything like digital photos, digital videos, audio files and text files. The final component is the stego message which is as crucial as the secret message. The stego message component refers to the final product. With the characters and important application, digital watermarking technology has been got more and more attention. In the future the main application of this technique is: copyright protection, pirate tracking, copying protection, image authentication, cover-up communication, classification control of digital watermarking video and so on. And the common characters of digital steganography is: insensitivity, secrecy, robustness and insurance. According to the different partitions, watermark can be parted in different types like these: significant watermark and the insignificant; the visible and the invisible; the brittle and the steady; the spatial domain watermark and the transformed domain watermark; the blind, the semi blind and the nonblind. One another partition is carrier and there are image watermark, audio watermark, video watermark, text watermark.

DCT coefficients are used for JPEG compression. It separates the image into different parts of importance. It transforms a signal or image from the spatial domain to the frequency domain. It separates the image into high, middle and low frequency components. In low frequency sub- band, much of the signal energy lies at low frequency which contains most important visual parts of the image, while in high frequency sub- band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image is not affected.
With the character of discrete Fourier transform (DFT), discrete cosine transform (DCT) turn over the image edge to make the image transformed into the form of even function. It's one of the most common linear transformations in digital signal process technology.
Twodimensional discrete cosine transform (2D-DCT) is defined as

$$F(jk)=a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (1)$$

The corresponding inverse transformation
(Whether 2DIDCT) is defined as

$$f(mn)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (2)$$

The 2D-DCT can not only concentrate the main information of original image into the smallest low frequency coefficient, but also it can cause the image blocking effect being the smallest, which can realize the good compromise between the information centralizing and the computing complication. So it obtains the wide-spreading application in the compression coding.

Objective:

To hide text inside a carrier image using Discrete cosine transform and then applying inverse DCT, to get the hidden text back. The text is encrypted using blowfish algorithm for added security, so that in the off chance the text is identified in the image, the eve will not be able to make sense of this data. This is to be implemented in Python. Also, we capture data loss metrics such as Mean Square Error, Peak Signal to Noise ratio and Structural Similarity Index (SSIM) to estimate fidelity and to get a brief idea about the efficiency of the algorithm.

Problem Statement:

In frequency space, the picture is first changed to its frequency appropriation. Not at all like in the spatial area where changes are made to pixel esteems straightforwardly, in recurrence space the rate is managed at which the pixel esteems change in spatial area. Whatever preparing is to be done is conveyed in recurrence area and the resultant picture is exposed to opposite change to get the necessary picture. Discrete cosine change (DCT), discrete fourier change (DFT), discrete wavelet change (DWT) and so forth are the instances of recurrence area. Stegnography measure in change space proposed entropy based method utilizing block level entropy thresholding. In this technique, cover picture was partitioned into 8×8 non covering blocks. Subsequent to choosing block DCT was processed for chosen block. Secret message was installed on block by center recurrence choice. This technique gave a lot of best heartiness, great PSNR results and gives high security introduced recurrence area steganographic strategy dependent on entropy thresholding plan. In this strategy, enormous volume of information was inserted in picture. In the wake of registering 64 DCT coefficients for each non covering block, entropy of four most critical pieces and least huge pieces was processed. This proposed procedure was information concealing strategy with which one can change quality factor and implanting limit progressively.

Literature Review:

Cox et al. [1] noticed that all together for a watermark to be vigorous to assault, it should be set in perceptually huge spaces of the picture. The watermark depended on 1000 irregular examples of a N(0,1) appropriation. These examples were added to the 1000 biggest DCT coefficients of the first picture, and the opposite DCT was taken to recover the Watermark Transmission: Extract Signal Information Original Image I Watermark W Watermarked

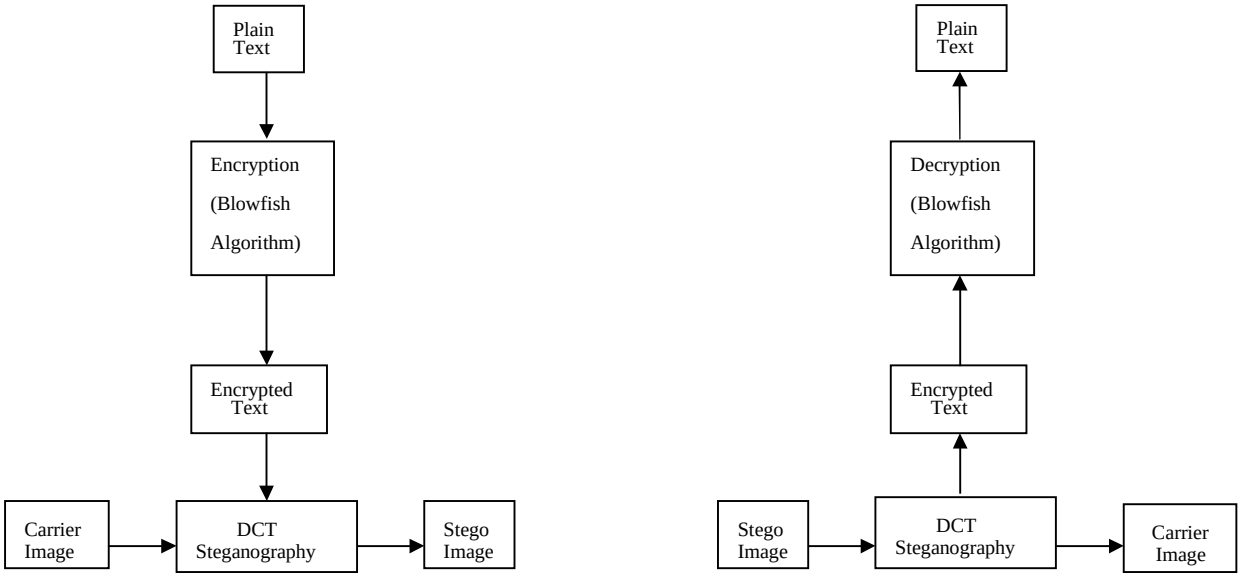
Picture I' Watermark Detection: Suspected Image J Compute Similarity Extract Watermark S>τ? Watermark distinguished, or Not identified, watermarked picture. For recognition, the watermark was removed from the DCT of a speculated picture. Extraction depended on information on the first sign and the specific recurrence areas of the watermark. The relationship coefficient was processed and set to a limit. On the off chance that the relationship was adequately huge, the watermark was identified. Their strategy was strong to picture scaling, JPEG coding, vacillating, editing, and rescanning.

Xia, Boncelet, and Arce [5] proposed a watermarking plan dependent on the Discrete Wavelet Transform (DWT). The watermark, demonstrated as Gaussian commotion, was added to the center and high recurrence groups of the picture. The deciphering cycle included taking the DWT of a conceivably stamped picture. Areas of the watermark were extricated and related with segments of the first watermark. In the event that the pass relationship was over a boundary, the watermark was recognized. Something else, the picture was disintegrated into better and better groups until the whole, removed watermark was connected with the whole, unique watermark. This strategy end up

being more vigorous than the DCT technique [1] when installed zero-tree wavelet pressure and halftoning were performed on the watermarked pictures.

Enhancements for the above plans were conceivable by using properties of the Human Visual System. Bartolini et al. [6] first created a watermarked picture from DCT coefficients. At that point spatial covering was performed on the new picture to conceal the watermark. Kundur and Hatzinakos [7] implanted the watermark in the wavelet area. The strength of the watermark was dictated by the difference affectability of the first picture. The two procedures showed protection from normal sign handling activities. Bas, Chassery, and Davoine [10] presented a watermarking framework utilizing fractal codes. A collection map was made from 8x8 squares out of the first picture and from the picture's DCT. The watermark was added to the arrangement guide to create a checked picture. Results showed that fractal coding in the DCT space performed better compared to coding in the spatial area. The DCT-based watermarking method was powerful to JPEG pressure, while spatial fractal coding created block ancient rarities after pressure.

System Model:



Algorithm to embed text message: -

Step 1: User inputs cover/carrier image.
Step 2: User inputs text message to be embedded in the image. This is then encrypted using blowfish algorithm. Key used is the password entered by user.
Step 3: The cover image is broken into 8×8 non-overlapping block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret text message. Step 8: Stego image is thus obtained.
Step 9: Calculate the Mean square Error (MSE), Peak Signal to Noise Ratio (PSNR) of the stego image to calculate fidelity.

Algorithm to retrieve text message: - Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 4: Inverse DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

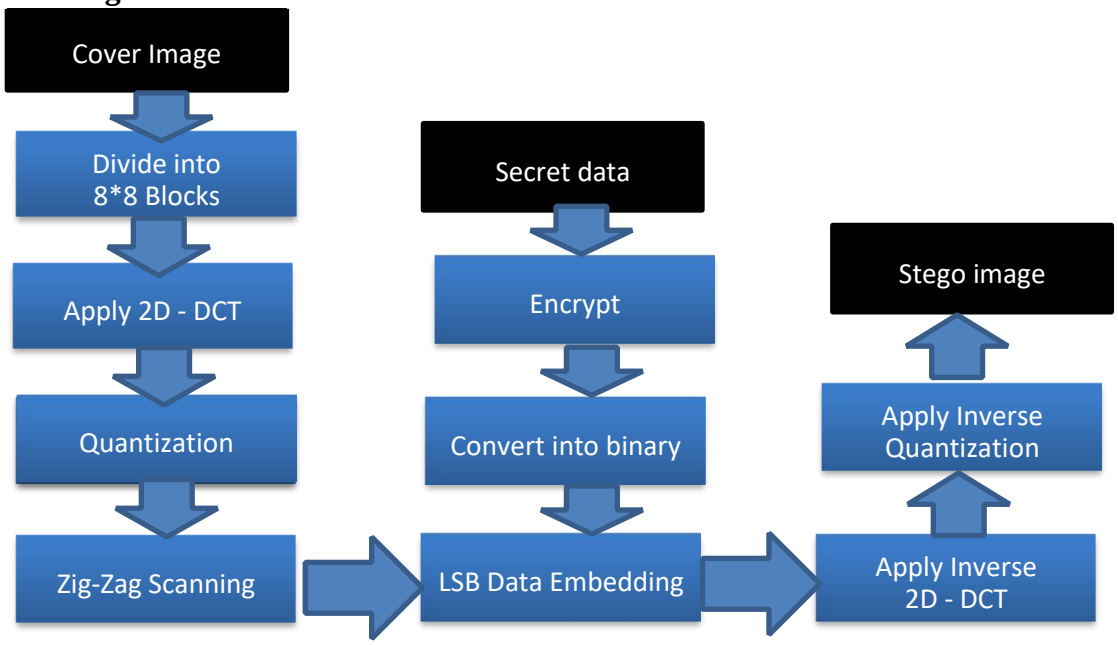
Step 8: Decrypt this encrypted text message using same password.

Step 9: Original text message is obtained.

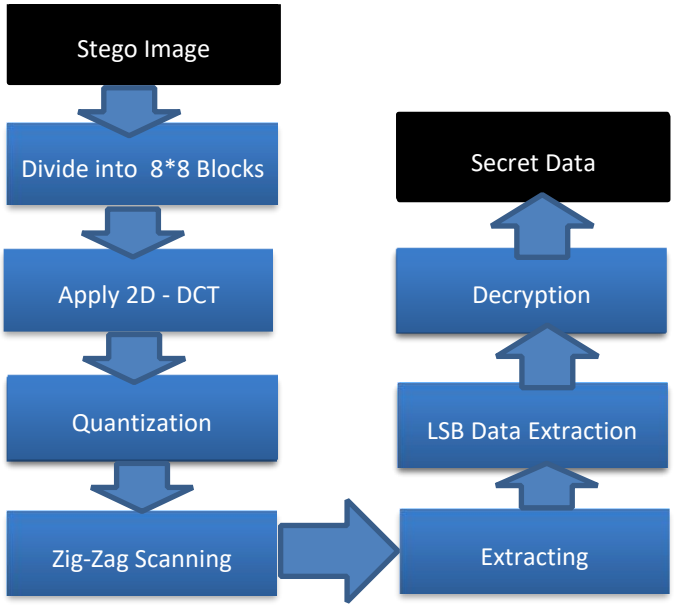
In depth Methodology:

1) Input cover image
2) Ensure the image dimensions are an integer multiple of 8 length-wise and height-wise.
3) If they aren't, the image is resized so that it can be evenly split into 8x8 pixel blocks.
4) After any necessary adjustments are made to the dimensions, the next step is to convert the color space from RGB to YUV, so the luminance (Y) layer is exposed. This is the layer intended for the data insertion as it is harder to notice the slight variations in luminosity
5) The user chooses a character string to embed into the cover image, which is then encrypted and converted into a binary representation and stored for embedding later.
6) Once the cover image has been properly segmented, it is transformed block-wise with the Forward DCT transform mentioned previously, and quantized by the JPEG quantization matrix. Once the DCT coefficients have been properly ordered by frequency content, the resultant matrix is then quantized in order to get integer values that are more reliable for data insertion. Once the frequency coefficients have been quantized, the embedding process can begin.
7) In order to determine which coefficients correspond to high low and medium coefficients, the transformed block is processed in what's called the 'zig-zag' pattern.
8) We select those medium frequency DCT coefficients to embed the secret data bits. Then the data is embedded into the LSB of the DCT coefficients.
9) Now the image is inversely transformed back into the spatial domain using inverse 2D DCT transform and is also dequantized, converted back into RGB channel and stitched together into the original dimensions. This is the stego image.
10) Now to extract secret message simply do the reverse process.

Embedding:



Extracting:



References:

[1] Mei Jiansheng, Li Sukang and Tan Xiaomei, ―A Digital Watermarking Algorithm Based On DCT and DWT‖ -Nanchang Institute of Technology, Nanchang, China

[2] Thottempudi Pardhu, Bhaskara Rao Perli ―Digital Image Watermarking in Frequency Domain‖ - International Conference on Communication and Signal Processing, April 6-8, 2016, India. [3] Saravanan Chandran, Koushik Bhattacharyya, ―Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography‖ - International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) - 2015.

[4] Gurmeet Kaurand Aarti Kochhar, ―A Steganography Implementation based on LSB & DCT‖, ―International Journal for Science and Emerging, Technologies with Latest Trends‖ 4(1), ISSN No. (Online):2250-3641, ISSN No. (Print): 2277-8136, 35-41 (2012).

[5] Neivin Mathew, Robyn Rintjema and Steven Kalapos, ―Comparison of Image Steganography Techniques (DCT vs LSB)‖

[6] Yashovardhan Kelkar and Heena Shaikh. Analysis of Robustness of Digital Watermarking Under Various Attacks. Special issues on IP Multimedia Communications (1):47-51, October 2011.

5. X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

6. F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454

D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 544-547.

P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473.