

# Steganography Using DCT And Wavelet Transform

S. Thenmozhy, Student, DR. S. J. S Paul, R.Suganya, DR. S. J. S Paul, S.Jayalakshmi, R. Rajasekar, DR. S. J. S Paul Memorial, DR. S. J. S Paul

Bachelor of Technology, Electronics and Communication Engineering,  
Memorial College of Engineering and Technology, Puducherry,India.  
Student, Bachelor of Technology, Electronics and Communication Engineering,  
Memorial College of Engineering and Technology, Puducherry,India.  
Asst. Prof. Bachelor of Technology, Electronics and Communication Bachelor of Technology, Electronics and Communication Engineering, College of Engineering and Technology, Puducherry,India.  
Memorial College of Engineering and Technology, Puducherry,India.  
Email ID: viji8292@gmail.com, sekarrajan22@gmail.com, thenmozhy1393@gmail.com, suganyar32@ymail.com

**Abstract:** Steganography is the technique used for communicating secret data. It is used for security purpose. The data can be image, video, aud io or text. We have kept secret data(image) under the cover image. In this work, we have used two algorithm one is DCT (Discret Cosine Transform) and the other one is Wavelet Transform.In DCT based technique insertion of secret information over the cover image depends upon the DCT coefficients. The main aim of our paper is to compare the PSNR value for DCT and Wavelet Transform. It is found that the PSNR value for DCT is better than the PSNR value for wavelet.

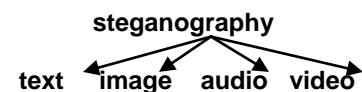
**Keywords:** DCT, Wavelet Transform, PSNR value, Steganography

## I. INTRODUCTION

Steganography usually focus on communicating secret data.The approach attempts to hide the image through the media. Rocha and Goldenstein described the applications of information hiding in various ways[4]. The straightforward application is in the military area where the secret communication is needed.In the medical imagenary,The patient information should be hidden in the medical image such as a radiological image or mammogram[5].So that the doctor will have the patient information at the same time.Also the quality of the image should not be degraded for examination.In the document tracking tool,the authorship of the document should be saved to state the owner of the document and for authentication.Many more applications can be found in[4]. There are number of aspects to be considered .First ,the media used for steganography should be selected.Second, The message(image) should be selected. Third the algorithim of combining the message(image)to the media should be selected. Criteria are considered for algorithms in the embedded processing such as the noises of the resulting stego media, the size of the stego media, the robustness of the algorithm through the compression of the stego media etc. In this steganography algorithm , we are using two ways of transformation such as DCT and Wavelet. The quality of the stego image in both selected algorithm are compared.The PSNR value are used to measure the quality of the stego images. Other aspects of comparison are considered in the future. The paper is organized as follows. Section 2 presents the steganography approaches. Section 3 presents the DCT based image coding. Section 4 presents the Wavelet based image coding. Section 5 presents the comparison results with some discussion.Section 6 concludes the work and presents the future work.

## II. STEGANOGRAPHY

Steganography is a type of hidden communication that literally means “covered writing” it’s from the Greek words stegano or “covered” and graphos or “to write”. The goal of Steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message. Oftentimes throughout history, encrypted messages have been intercepted but have not been decided. While this protects the information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place. Essentially, the information hiding process in a Steganography system start by identifying a cover medium’s redundant bits (those that can be modified without destroying that medium’s integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography goal is to keep its mere presence undetectable, but steganographic system, because of their invasive nature, leave behind detectable traces in the cover medium through modifying it’s statically properties. The process of finding these distortions is called statistical steganalysis.



The goal of Steganography is to embed a message in cover object in a covert manner such that the presence of the embedded in the intended recipient. Steganographic applications only require the flexibility to alter C in order to be able to embed the hidden information. For this reason any type of digital object can be potentially used as a cover. For example, images, audio, streaming data software or

natural language text have been used as cover objects. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

### III. DISCRETE COSINE TRANSFORM

Transform coding constitutes an integral component of contemporary image/video processing applications. Transform coding relies on the premise that pixels in an image exhibit a certain level of correlation with their neighboring pixels. Similarly in a video transmission system, adjacent pixels in consecutive frames show very high correlation. Consequently, these correlations can be exploited to predict the value of a pixel from its respective neighbors. A transformation is, therefore, defined to map this spatial (correlated) data into transformed (uncorrelated) coefficients. Clearly, the transformation should utilize the fact that the information content of an individual pixel is relatively small i.e., to a large extent visual contribution of a pixel can be predicted using its neighbors. A typical image/video transmission system is outlined. The objective of the source encoder is to exploit the redundancies in image data to provide compression. In other words, the source encoder reduces the entropy, which in our case means decrease in the average number of bits required to represent the image. On the contrary, the channel encoder adds redundancy to the output of the source encoder in order to enhance the reliability of the transmission. Clearly, both these high-level block have contradictory objectives and their interplay is an active research area. However, discussion on joint source channel coding is out of the scope of this document and this document mainly focuses on the transformation block in the source encoder. A **discrete cosine transform (DCT)** expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from loss compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions. A much

better transform, from this point of view, is the DCT in this example we see the amplitude spectra of the image above under the DCT. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT", its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sines transform (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosines transform (MDCT), which is based on a DCT of overlapping data. Lin and Shiu proposed to use DCT for data hiding in cover image [9]. The data is hidden in the DCT coefficients. Abed and Mustafa proposed to combine between steganography and cryptography that can hide a text in an image in a way. They developed the application which embeds the text to the image. Their approach is based on DCT and give the PSNR value about 28-30 dB on the sample image [10]. Hashad et.al presented to use LSB insertion bit to high data and then combine with the DCT transform [11].

### IV. WAVELET TRANSFORM

Wavelet transforms have become one of the most important and powerful tool of signal representation. Nowadays, it has been used in image processing data compression, and signal processing. In order to analyze signals of very different sizes, it is necessary to use time-frequency atoms with different time supports. The wavelet transform decomposes signals over dilated and translated functions called wavelets, which transform a continuous function into a highly redundant function. When we listen to music, we clearly hear the time variation of the sound frequencies. The properties of sounds are revealed by transforms that decompose signals over elementary functions that are well concentrated in time and frequency. Windowed Fourier transforms and wavelet transforms are two important classes of local time-frequency decompositions. A linear time-frequency transform correlates the signal with a family of waveforms that are well concentrated in time and in frequency. These waveforms are called time-frequency atoms. Reddy and Raja proposed to use the discrete wavelet transform (HCSSD) [6]. The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters, alpha and beta. The cover and payload are preprocessed to reduce the pixel range to ensure the payload are preprocessed to reduce the pixel range to ensure the payload is recovered accurately at the destination. Ali and Fawzi [7] used the 2D wavelet transformation on the image and encrypted the message using RC4 algorithm with the payload of 73%, the approach can yield PSNR at 22.84dB. Safy et.al proposed the adaptive approach where the message is hidden in the wavelet coefficients with the optimum pixel adjustment selection [8]. The approach selects the random coefficients for further security.

## V. COMPARISON OF DCT AND WAVELET TRANSFORM

In this paper, we select to study the steganography algorithms. The two particular transformations are considered in the frequency domain. They are DCT and Wavelet transform. Our test framework is based on the following steps.

**Input:** input image, cover image.

**Output:** Stego image.

Aspects	Wavelet based algorithm[7]	DCT based algorithm[10]
Transformation	Wavelet	DCT
Size of block to transform	MxN	(MxN)/64
Number of times to transform	1	p
Iteration used to search to space to hide	At most O(MxN)	O(px((MxN)/64))
Methods to search for hiding position	Position has less than threshold value	Always at(1,1) position of (8,8) block

### A. DCT based algorithm[10]

The DCT based algorithm is obtained from[10]. The algorithm is described as following

- Select the carrier image
- find DCT coefficients of carrier image
- Traverse through each pixel in carrier image till end of secret image.
- If DCT coefficient value is below threshold then replace LSB with MSB of pixels in secret image.
- Insert 1 at that location in the key matrix.
- Evaluate the Stego image.

### B. Wavelet based algorithm [7]







The Wavelet based algorithm is obtained from [7]. The algorithm is described as follows.

- Divide the cover image into 4\*4blocks.
- Find the frequency domain representation of blocks by 2D Haar Wavelet transform and get 4 sub bands LL1, HL1, LH1, and HH1.
- Generate 16 genes containing the pixel no in each block as mapping function.
- Embed the message bit in k-LSBs DWT coefficients each pixel according to mapping function.
- Fitness evaluation is performed to select best mapping function.
- Apply optimal pixel adjustment process in image.

Comparing between the cover image C and the resulting stego image S using Root mean Square Error (RMSE) =  $\sqrt{\text{mean}((S-C)^2)}$  and Peak Signal to Noise Ratio (PSNR) =  $20 \log(255/\text{RMSE})$ .

## IV. CONCLUSION

It is concluded that the PSNR value for both Discrete Cosine Transform and Wavelet transform is given .Hence this PSNR value for wavelet transform is less than PSNR value for discrete cosine transform. So that error occurrence can be reduced. Hence DCT transform is better than wavelet transform.

Cover image	Secret image	PSNR	
		DCT	WAVELET
		32.34	23.765
		31.74	22.65
		34.67	20.34

## REFERENCE:

- [1] A chedded, J.Condell,K Curran, and P. McKeVitt, "Digital image steganography: survey and analysis of current methods", signal processing, vol.90,pp.727-752,2010.
- [2] N. Hamid, A. Yahya, R B.Ahmad and Osamah M. Al-Qershi "Image steganography techniques: an overview International journal of computer science and security(IJCSS),Vol.6, No. 3, 2012.
- [3] T. Morkel, JHP. Eloff and MS. Olivier, "An Overview An overview of image steganography," in HS Venter, JHP Eloff, L Labuschagne and MM Eloff(eds), Proceedings of the fifth annual information security south Africa conference (ISSA2005), Sandton, south Africa, june/july 2005 (published electronically).
- [4] A.Rocha, and S. Goldenstein,"Steganography and steganalysis in multimedia : hype or hallelujah?", RITA, Vol. 15, No. 1, 2008.
- [5] C. -T. Li, Y. Li, and C.H. Wei, "Protection of digital mammograms on PACSs using data hiding technique", International journal of Digital Crime and Forensics , Vol. 1, No.1, pp. 75-88.
- [6] H. S. Majunatha Reddy, and K. B. Raja, "High capacity and security steganograph using wavelet transform", International journal of computer science and security (IJCSS), Vol. 3, issues 6, 2010, 462-472.

- [7] A-A. Ali and A-N. Fawzi , “ A modified high capacity image steganography technique based on wavelet transform”, The international arab journal of information technology, Vol. 7, No. 4, October 2010, pp.358-364.
- [8] R. O.E1 Safy, H. H. Zayed, and A. E. Dessiouki, “An adaptive steganographic technique based on integer wavelet transform”, International conference on networking and media convergence (ICNMM 2009), pp.111-117, March 2009 doi: 10.1109/ICNM.2009.4907200.
- [9] C,-C. Lin, and P.-F.SHIU, ”High Capacity Data Hiding Scheme for DCT- basedImages”, Journal of Information Hiding and Multimedia Signal Processing 2010 ISSN 2073-4212, Ubiquitous International, Vol 1, No.3, July 2010.
- [10] F. S. Abed, N.A. A. Mustafa, ”A Proposed Technique for Information Hiding Based on DCT”, International Journal of Advancements in Computing Technology Vol. 2, No.5, December 2010, pp.140-152.