Analysis of Frequency Domain Image Steganography using DCT and DWT

Jagdish Bhatta[1], Sajina Maharjan[1], Dhiraj Kedar Pandey*[1], Binit Lekhak[2]
[1]Central Department of Computer Science and IT, Tribhuvan University
[2]Kathmandu Model College
*Corresponding Author: Dhiraj Kedar Pandey (dhiraj@cdcsit.edu.np)

Keywords
Image Steganography, Discrete Cosine Transformation, Discrete Wavelet Transformation, Security

Received: 1 November 2025
Revised: 28 November 2025
Accepted: 3 December 2025

ISSN: 3059 - 9687

Copyright: @Author(s) 2024

Abstract

Steganography is a way of hiding messages during communication within some cover media. Image Steganography the process of hiding secret messages in a cover image. Frequency domain hides the secret bits of input message within the significant parts of the cover image. It encodes bits of the message into the transform domain coefficients of the image. Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) come under frequency domain technique. This research evaluates the DCT, DWT and a hybrid DCT with DWT algorithms using four measures Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Number of Pixel Change Rate (NPCR), and histogram. The result shows that DCT with DWT is better than the two algorithms DCT and DWT. The PSNR value of the combined method has the highest value of the other two techniques. DCT with DWT preserves the originality of input image and the stego image without losing image properties. The average PSNR value for DCT with DWT is 77.59, DWT is 71.07 and DCT is 73.08 and it signifies DCT with DWT is better. The average encoding and decoding time for DCT with DWT is 0.15, DWT is 0.43 and DCT is 0.46. Thus DCT with DWT being feasible for computational point of view. The differential analysis values for DCT with DWT, DWT and DCT with an average of NPCR are 92.60%, 91.56% and 91.43% respectively. All of the three algorithms are found to be good on histogram analysis producing similar histogram distributions of input and stego images.

Introduction

The massive growth in the information technology and internet has made the distribution of digital content very easy and at low cost. However this advancement has also brought a number of security threats like unauthorized access and modifications on the contents. Even though there are cryptographic mechanisms to maintain integrity and security of information, they deal by message encryption with a condition that the communication is visible and suspicious to attackers (Albderi et al., 2023). There is a need for concealment of messages using a concept known as steganography. An increased level of protection is provided by the steganography technology, which conceals the message's existence so that intruders cannot determine what communication is taking place. Three components make up a steganography system: the cover image, which conceals the secret message, the secret message, and the stego image, which is the cover object with the message embedded in it (Vijayarajeswari et al., 2016). Since the structure of images is more complex than that of text data, employing image files to conceal information has the advantage of creating a lot of extra space for storing the information and adding security against hacker attacks. Image steganography can work in spatial domain and frequency domain. Spatial domain techniques embed messages in the intensity of pixels directly. Mathematically, a digital image is a 2D matrix of the color intensities at each pixel. The gray images use 8 bits, whereas the RGB model utilizes 24 bits to describe the color model (Rathi, 2024).

There are various ways to hide information behind the cover image in an image steganography system that employs an image as the cover. Some of them are based on the frequency domain, while others are based on the spatial domain. To incorporate the secret information, spatial domain approaches change the cover image pixel bit values (Trivedi et al., 2016). The cover image pixel bytes are directly written with the secret bits. The spatial domain approaches are therefore straightforward and simple to use. One of the primary methods in spatial domain image steganography is the Least Significant Bit (LSB) (Jung, 2018). Spatial domain techniques either operate on pixel wise or block wise bases. The advantage of the method is that the amount of data that can be embedded is more in LSB techniques. Spatial approaches are susceptible to all watermarking attacks as well as rotating, cropping, and scaling assaults. These embedding methods work best with lossless image-compression strategies such as TIFF images. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step (Lakshmi & Chandra, 2021). Thus the frequency domain is processed to overcome the shortcoming of LSB i.e. weak resistance to attacks. In this method, pixel values are transformed and those transformed coefficients are used for processing (Abdirashid et al., 2022). The frequency domain hides the secret bits of message in the key regions of the cover image. It attempts to insert message bits in the transform domain coefficients of the image. The frequency domain includes Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT) (Sharma & Sharma, 2018).

Determining the impact of embedding the secret messages into various bands of the cover image is crucial because the frequency techniques involve converting the cover image into the frequency domain coefficients prior to embedding hidden messages.In this context, evaluating the performance of the frequency domain methods viz. DCT, DWT and DCT with DWT by the image quality and imperceptibility is the focused problem of this study.

Materials And Methods

Embedding Text using Discrete Cosine Transformation (DCT)

In Discrete Cosine Transformation, for each color component the JPEG image format uses a discrete cosine transform to transform successive 8×8 pixel blocks of the image into 64 DCT coefficients each (Bansal & Chhikara, 2014). The DCT coefficients f(u, v) of an 8 x 8 block of image pixels f(x, y) are given by

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

Where, p(x, y) defines the $(x, y)^{th}$ element of the image in the image matrix p. N is the size of the block for DCT.For a standard 8×8 block, N is 8 and x, y belongs from 0 to 7.

From the pixel values of the original image matrix, equation (1) computes each (i, j) of the converted image. Because the DCT uses the cosine function, the resulting matrix depends on the horizontal, diagonal, and vertical frequencies. (Ayub & Selwal, 2020).

The cover image is read and split into 8 × 8 pixel blocks in order to include the message bits. The image block is subtracted from 128 from each entry since DCT is designed to work on pixel values ranging from -128 to 127. Then on the resultant matrix the DCT is performed, which is accomplished by matrix multiplication.

$$D = T\,M\,T' \tag{2}$$

Where, M is shifted image block, T' is transpose of T and T is DCT matrix which is obtained from following equation

$$T_{i,j} = 1/\sqrt{N} \text{ if } i=0 \tag{3}$$

$$\sqrt{(\tfrac{1}{N})}\, cos\, cos \left[\frac{(2j+1)i\Pi}{2N}\right] \text{ If } i>0$$

The 8 × 8 block of DCT coefficient is compressed by quantization. During quantization the less important frequencies are discarded. Quantized DCT blocks are created by dividing each element in the adjusted image matrix by the corresponding element in the quantization matrix. These blocks are then rounded to the nearest integer value.Standard quantization matrix Q is employed for this.(Bansal & Chhikara, 2014). After obtaining quantized DCT blocks, the LSB of each DC coefficient is calculated and replaced with each bit of the secret message. The zero element is discarded and only the non-zero element is taken to embed the message using LSB. Dequantization is achieved by multiplying each element of the transformed matrix after secret message hiding by corresponding element in the quantization matrix. For this the same quantization matrix Q is used. The matrix is then rounded to the closest integer and subjected to the inverse DCT. The JPEG version N of the original 8 x 8 image block is obtained by adding 128 to each element of that result. The stego image is recreated by merging the 8 x 8 image blocks.

Embedding Text Using Discrete Wavelet Transformation (DWT)

Wavelets are special functions which are used as basal functions for representing signals (Fakhredanesh et al., 2019). During this study, the most basic discrete wavelet transform (DWT), Haar-DWT is used. In Haar-DWT, high frequency wavelet coefficients are produced by taking half of the difference between the same two pixels, whereas low frequency wavelet coefficients are produced by averaging the two pixel values.(Houssein et al., 2016).

Applying the Discrete Wavelet Transform to 2D image divides the image into horizontal (HL), vertical (LH), and diagonal (HH) detail components and a lower resolution approximation image band (LL). With the DWT, the edge and texture details typically appear in high frequency subbands like HH, HL, and LH, while the substantial and smooth portions of the spatial domain image are found in the approximation band made up of low frequency wavelet coefficients i.e. LL. (Narasimmalou & Allen, 2012).

For a 2 × 2 pixel block of an image represented as$\begin{pmatrix} x1 & y1 \\ x2 & y2 \end{pmatrix}$, the low pass and high pass are defined as;

$$L = \frac{x1+y1}{2}\,;\; H = \frac{x2-y2}{2} \tag{4}$$

The approximation, horizontal, vertical and diagonal components are defined as;

$$LL = \frac{(x1+y1)+(x2+y2)}{4} \tag{5}$$

$$LH = \frac{(x1-y1)+(x2-y2)}{4} \tag{6}$$

$$HL = \frac{(x1+x2)-(x2+y2)}{4} \tag{7}$$

$$HH = \frac{(x1-y1)-(x2-y2)}{4} \tag{8}$$

To embed the secret message using DWT the cover image is taken and decomposed into three color planes i.e. red, green, and blue. The red plane is considered. By applying Haar DWT, it is divided into four sub bands. Pixels are scanned horizontally from left to right in order to apply Haar DWT. Next, neighboring pixels are subjected to addition and subtraction processes. The difference is kept on the right, and the sum is kept on the left. Until every row has been processed, this process is repeated. The low frequency portion of the original image, shown by L, is represented by the pixel sum, and the high frequency portion, indicated by H, is represented by the pixel difference.

Once more, the pixels are scanned vertically from top to bottom. Neighboring pixels undergo addition and subtraction processes. The difference is kept at the bottom and the sum at the top. Until every column has been processed, this process is repeated. Four subbands namely LL, HL, LH, and HH are ultimately produced by this method. Here, LH is the difference of left top down pixels, HH is the difference of right top down pixels, LL is the total of left top down pixels, and HL is the total of right top down pixels. The binary bits of the secret message are then used to compute and alter the LSB of the HH sub band. The stego picture is then obtained by applying the inverse DWT and concatenating it with the plane.

Embedding Text Using DCT with DWT

This is a hybrid method of the DCT and DWT. In this method the cover image is divided into three color planes and divides the red plane into four sub bands using DWT. DWT splits the signal in low and high frequency parts. The high frequency part contains the information about the edge component so DCT is applied in HH band only. Since the human eye is less sensitive to changes in edges, high frequency components are typically utilized. (Kumar & Kumar, 2018).

Initially, the cover image is taken and divided into three color planes. DWT is applied in the red plane and divided into four sub bands. Then DCT is applied on the HH band of the red pane. The bits of the DCT coefficients of the aforementioned chosen subband are altered with bits of the secret message using LSB. The inverse Discrete Cosine Transform on the HH sub band is applied. After embedding bits of secret message in the red plane inverse wavelet transformation is applied to get back the plane. Finally each plane is concatenated to get a color stego image. In this research LSB is used to embed the secret message bit in the DC coefficient of HH sub band.

Performance Evaluation Parameters

The performance of the image steganography algorithms are evaluated using Peak Signal to Noise Ratio(PSNR), Mean Square Error (MSE), Number of Pixel Change Rate (NPCR) and the histograms. (Kombrink et al., 2025).

In Steganography technique, the signal is the maximum possible pixel value and noise is the error or change in image pixel value after embedding a secret message in it. It measure the quality of image between the cover image f and stego image g of size M*N. It is defined as follows:

$$PSNR = 10 * \frac{MAX^2}{MSE} \tag{9}$$

MSE measures the average square of error, i.e. noise or change in image introduced after embedding a secret message in it, between cover image and stego image.

$$MSE = \frac{1}{MN} \sum_{X=0}^{M-1} \sum_{Y=0}^{N-1} ((F(X,Y) - G(X,Y))^2 \tag{10}$$

Where, F(X, Y) represents the cover image and G(X, Y) represents the stego image.

NPCR measures the percentage of different pixel numbers between the cover image and stego image.

$$NPCR = \frac{1}{XY} \sum K(X,Y) \tag{11}$$

Assuming $K_1(i, j)$ be the cover image and $K_2(i, j)$ be the stego image. Then, K(i, j)=1, if K1(i, j)=K2(i, j) else it is 0.

Implementation and Experimental Setup:

The algorithms has been implemented using MATLAB R2016 in Windows with 2.5 GHz Intel core i5 processor and 8GB RAM.

Data Set Description

The input data for the experiment are the different standard images like Lena, Peppers, Baboon, of different dimensions like 256 × 256, 512 × 512 collected from USC-SIPI Image Database (SIPI Image Database, n.d.).

RESULTS AND DISCUSSION

Visual Assessment Analysis

PSNR and MSE are used to perform visual assessment analysis of the algorithms. The results are as below;

Table 1: Results of MSE and PSNR

S.N.	Image	Dimension	Method	MSE (dB)	PSNR (dB)
1.	Baboon.jpg	256*256	DCT	14.749344	72.886153
			DCT with DWT	6.369904	80.178950
			DWT	18.023007	64.512242
2.	Lena.jpg	512*512	DCT	14.182571	72.080657
			DCT with DWT	7.926361	78.280130
			DWT	13.002331	74.455644
3.	Pepper.jpg	512*512	DCT	12.567455	74.276660
			DCT with DWT	12.516895	74.311675
			DWT	12.542442	74.253509

It is observed that the DCT with DWT results better PSNR than the other two models indicating that the changes made to the cover image are minimal thus resulting in a stego image which is visually indistinguishable from the original image in comparison to the stego images from other two methods.

Computational Analysis

To perform computational analysis, the values of encoding and decoding time for different sets of images are computed in seconds. The encoding and decoding time of different methods are shown below:

Table 2: Results of Encoding and Decoding Time in Seconds

S.N.	Image	Dimension	Method	Encoding Time (s)	Decoding Time (s)
1.	Baboon.jpg	256*256	DCT	0.272815	0.094626
			DCT with DWT	0.069036	0.031078
			DWT	0.378932	0.038033
2.	Lena.jpg	512*512	DCT	0.874043	0.374802
			DCT with DWT	0.269972	0.120445
			DWT	0.889540	0.075235
3.	Pepper.jpg	512* 512	DCT	0.789885	0.376081
			DCT with DWT	0.299634	0.143299
			DWT	0.803443	0.395902

The above result clarifies that DCT with DWT is computationally efficient since the encoding and decoding time for DCT with DWT is minimal for all dimensions of the input data images.

Differential Analysis

Differential analysis is done for security measures. It is a technique which observes how difference in input affects differences on the output. NPCR is used to determine the difference. The results for NPCR are illustrated below;

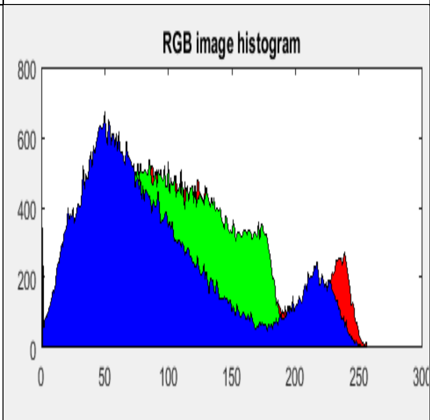
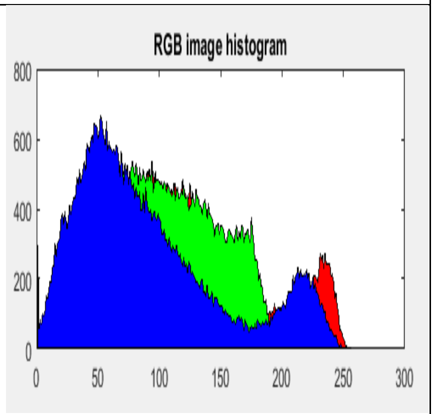
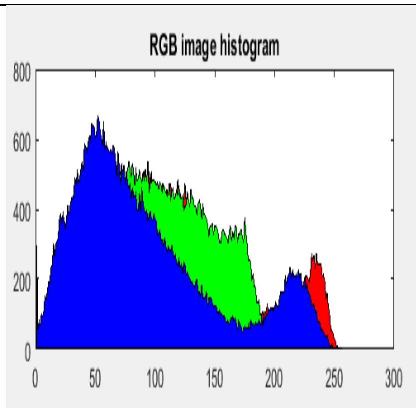
Table 3: Results of NPCR

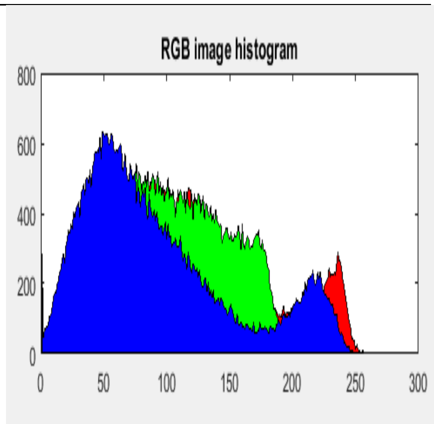
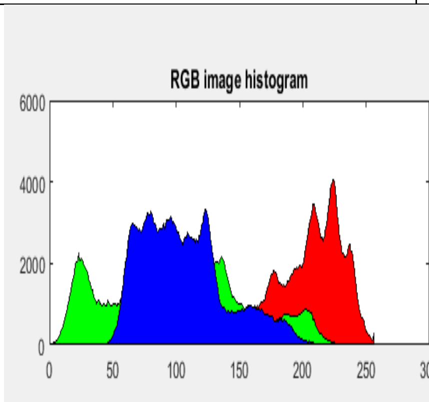
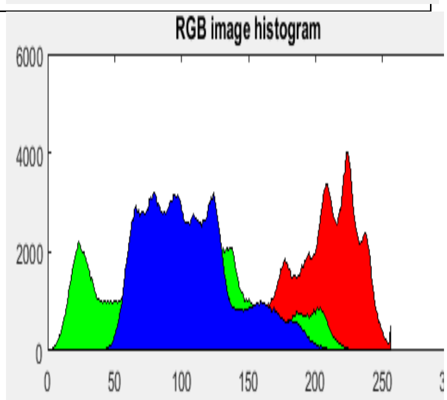
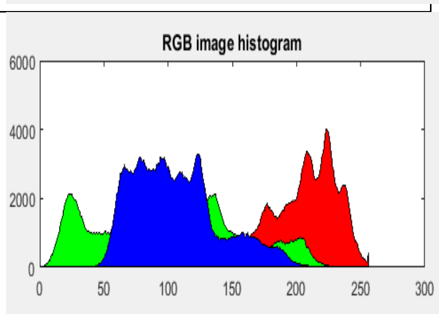
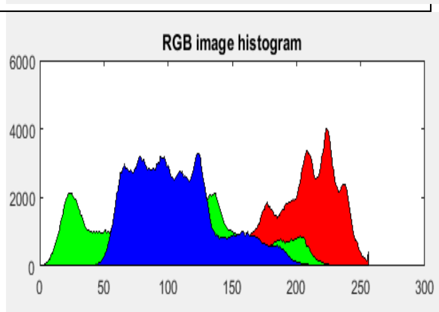
S.N.	Image	Dimension	Method	NPCR (%)
1.	Baboon.jpg	256*256	DCT	90.895081
			DCT with DWT	91.515747
			DWT	90.237427
2.	Lena.jpg	512*512	DCT	92.101669
			DCT with DWT	93.108627
			DWT	92.863846
3.	Pepper.jpg	512* 512	DCT	91.300964
			DCT with DWT	93.186325
			DWT	91.600418

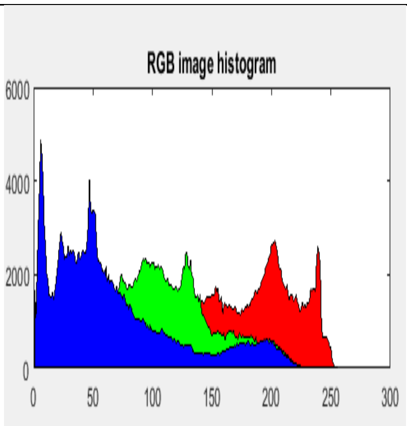
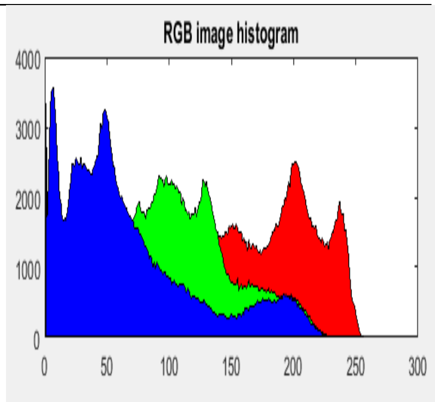
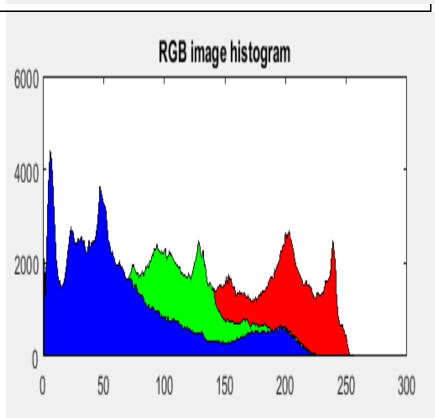
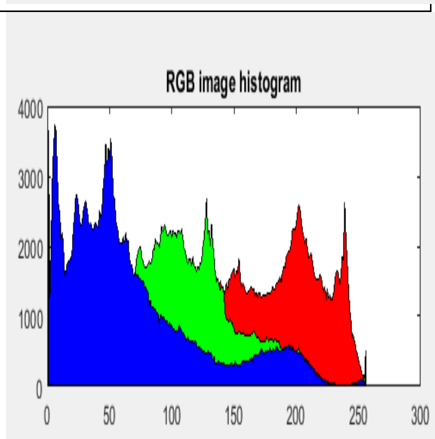
The DCT with DWT has good differential analysis values. This value is able to protect the image from attackers as it hides the significant information of image data since the net pixel change rate is higher.

Statistical Analysis

Statistical analysis is done for steganalysis using histograms. The histograms are used to check if statistical properties of an image vary after embedding any information in the image (Cheng et al., 2018; Vijayalakshmi et al., 2010). The histogram of different input and stegoimages generated during the experimentation are as follows:

S.N.	Image	Original Image histogram	Method	Stego Image Histogram
1.	Baboon.jpg		DCT	
			DCT With DWT	

			DWT	
2	Lena. Jpg		DCT	
			DCT With DWT	
			DWT	

3	Pepper.jpg		DCT	
			DCT With DWT	
			DWT	

The histograms that are obtained for the stego images from DCT, DWT and DCT with DWT method are almost identical as the difference due to steganographic embedding is extremely small. Thus resisting the statistical attacks.

The overall analysis shows that DCT with DWT method is computationally efficient with other two approaches. The PSNR value results show that DCT with DWT has maintained the image quality after encoding the secret message into cover image than other two approaches. Similarly, the DCT with

DWT has good differential analysis values with reference to the NPCR, hence resisting differential attacks. There is no significant difference in original cover image and stego image as the histograms of both images are almost identical, the algorithms ensure the secret message doesn't alter the tonal distribution.

Conclusion

Steganography is the need of today's digital world since there is no reliability over the medium through which the information is sent in computer networks. In other words the digital communication medium is not secured. So, some methods are needed so that it becomes difficult for unintended users to extract the information from the message sent secretly over the medium. Steganography is one of the solutions. In this study, steganography is done using DCT and DWT based algorithms. The images of different types are used for testing the strength of the algorithms. The algorithms are implemented and analyzed with different parameters to test the strength of the algorithm and found that DCT with DWT is better than other two algorithms as it has better PSNR value which also shows that it preserves the image quality after hiding secret messages. DCT with DWT is found to be computationally efficient as it takes less encoding and decoding time than other two methods. DCT with DWT has better NPCR values which verifies the strength of the algorithm in resisting differential attack. All of the three algorithms are found good against statistical attack in steganalysis.

References

Abdirashid, A. M., Solak, S., &Sahu, A. K. (2022). Data hiding based on frequency domain image steganography. *European Journal of Science and Technology*, (42), 71–76.

Albderi, A. J. T., Said, L. B., & Al-Shammary, D. (2023). Literature review for health secure image steganography and visual encryption. *2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT)*, 218–223. IEEE.

Ayub, N., &Selwal, A. (2020). An improved image steganography technique using edge based data hiding in DCT domain. *Journal of Interdisciplinary Mathematics*, *23*(2), 357–366.

Bansal, D., &Chhikara, R. (2014). An improved DCT based steganography technique. *International Journal of Computer Applications*, *102*(14).

Cheng, J., Chen, Z., & Yang, R. (2018). An efficient histogram-preserving steganography based on block. *EURASIP Journal on Image and Video Processing*, *2018*(1), 74.

Fakhredanesh, M., Rahmati, M., &Safabakhsh, R. (2019). Steganography in discrete wavelet transform based on human visual system and cover model. *Multimedia Tools and Applications*, *78*(13), 18475–18502.

Houssein, E. H., Ali, M. A. S., &Hassanien, A. E. (2016). An image steganography algorithm using haar discrete wavelet transform with advanced encryption system. *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 641–644. IEEE.

Jung, K.-H. (2018). Comparative histogram analysis of LSB-based image steganography. *WSEAS Trans. Syst. Control*, *13*(1), 103–112.

Kombrink, M. H., Geradts, Z. J. M. H., & Hubert, M. (2025). Image steganography approaches and their detection strategies: A Survey. *ACM COMPUTING SURVEYS*, *57*(2).

Kumar, V., & Kumar, D. (2018). A modified DWT-based image steganography technique. *Multimedia Tools and Applications*, *77*(11), 13279–13308.

Lakshmi Sirisha, B., & Chandra Mohan, B. (2021). Review on spatial domain image steganography techniques. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1873–1883.

Narasimmalou, T., & Allen, J. R. (2012). Optimized discrete wavelet transform based steganography. *2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 88–91. IEEE.

Rathi, H. (2024). Hiding information using image steganography. *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, *1*, 1–5. IEEE.

Sharma, P., & Sharma, A. (2018). Robust technique for steganography on red component using 3-DWT-DCT transform. *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 1049–1054. IEEE.

SIPI Image Database. (n.d.). Sipi.usc.edu. https://sipi.usc.edu/database/

Trivedi, M. C., Sharma, S., &Yadav, V. K. (2016). Analysis of several image steganography techniques in spatial domain: A survey. *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, 1–7.

Vijayalakshmi, D., Zayaraz, D., &Nagaraj, V. (2010). An image steganography algorithm against histogram and statistical analysis. *Networking And Communication Engineering*, *2*(2), 42-49.

Vijayarajeswari, R., Rajivkannan, A., Santhosh, J. (2016). A simple steganography algorithm based on lossless compression technique in WSN. *Circuits and Systems*, *7*(08), 1341-1351

.