Performance Evaluation of LSB, DCT AND DWT Steganography Algorithm

[1]Sadiq Aliyu Ahmad, [2]Dr. Maharazu Mamman, [3]Dr. Muhammad Sirajo Aliyu, [3]Prof. Ahmed Baita Garko

[1]ICT Directorate,
Federal University Dutse

[2]Department of Computer Science,
Federal College of Education Katsina

[3]Department of Computer Science
Faculty of Computing
Federal University Dutse

Corresponding Author: sadiqaliyu@fud.edu.ng

Abstract
The Internet is increasingly being used to transmit sensitive and confidential information. Several existing models to secure the internet are robust and secure, but more research is needed to make them safer and more secure in terms of performance measurements. Steganography techniques have been developed to overcome the shortcomings of cryptography techniques. In this research, the performance of three steganography algorithms (LSB, DCT, and DWT) were evaluated based on efficiency, compression and image quality. The steganography algorithms were implemented using Python, and three different cover images were used to hide secret messages. Finally, the algorithms were analyzed using the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) measures. The results showed that while DCT and DWT were more efficient in terms of compression ratio, LSB was more efficient in terms of MSE and PSNR, indicating that LSB is more efficient and may be more suitable for certain applications.

Keywords: Data Security, Steganography, LSB, DCT, DWT, MSE, PSNR

INTRODUCTION

People are increasingly using the Internet to convey sensitive and confidential information. Advances in digital communication play an important part in modern life. Several existing strategies are robust and secure, but research is still being done to make them safer and more secure in terms of performance measurements. Several studies have been conducted to investigate data security. [1]. Although the existing studies are robust and secure, more research are ongoing to make these approaches safer and more secure in terms of performance measures. Steganography techniques have been developed to overcome the weaknesses of cryptography techniques. The steganography technique is used to hide data behind other media content or files. Steganography is the process of hiding data in coded media files such as

images, audio, text, and video. It is a tool that preserves data and secret information that can only be detected by the sender and its respective receiver [2].

Steganography

Steganography is the art and science of using digital communication objects in such a way that the existence of secret information is concealed. The core process of steganography is data embedding and retrieval. For embedding, cover media and encryption keys are sent to the embedding algorithm, which then provides the stego media with secret information. After the data is transferred, it is recovered at the recipient using the exact same technique as when it was embedded. For proper retrieval, the keys used during embedding should be available at the receiver side. [3]

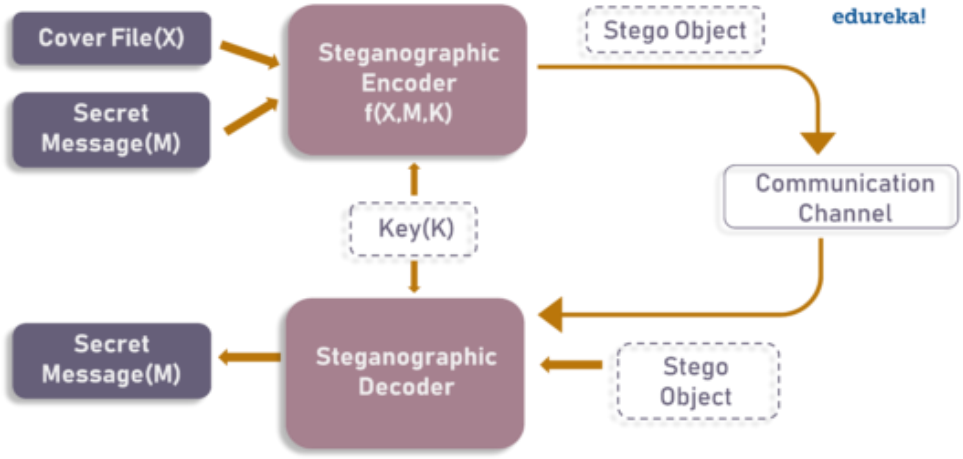

Figure 1 Steganography Technique [1]

Steganography Techniques

Steganography is classified into five forms based on the nature of the cover item (the actual thing in which the secret data is embedded) the figure 1 above shows the steganography technique:

A. **Text Steganography:** Text steganography is the practice of hiding data within text files. It involves modifying the format of existing text, changing words within a document, generating random letter sequences, or constructing readable texts using context-free grammars. Among the several approaches used to hide facts in text are:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

B. **Image Steganography:** Image steganography is the technique of hiding data by using the cover object as the image. Images are a popular cover source in digital steganography because the digital representation of an image contains many bits. There are numerous methods for concealing information within an image. Image steganographic algorithms can be classified into two main classes: [4]

Spatial domain algorithms: These methods insert the secret text directly on the cover image using the embedding process. These algorithms are simple and fast, but they are vulnerable to distortions and compression. They use techniques such as Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Exploiting Modification Direction (EMD). [4]

Transform domain algorithms: Transform domain algorithms change the cover picture into another format before applying the embedding procedure to the new format. These algorithms are resistant to distortion and compression, but they are computationally expensive. They adopt techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Fast Fourier Transform (FFT). [4]

C. **Video Steganography:** Video steganography is a branch of data hiding, which is a technique that embeds message into cover contents and is used in many fields such as medical systems, law enforcement, copyright protection and access control, etc. [5]

D. **Audio Steganography:** Audio steganography is a technique for hiding information in audio by taking advantage of weaknesses in the human auditory system. Audio steganography is more difficult than image steganography, which is perceptually undetectable to the user. The quality of sound may be affected if audio bits are changed. A successful audio steganography may provide an output that is comparable to the original audio and cannot be detected by the human ear. LSB is a technique used to conceal information in digital audio. The secret message's characters are converted into binary values. The Least Significant Bit technique is then used to embed each message bit into digitized cover audio. [6]

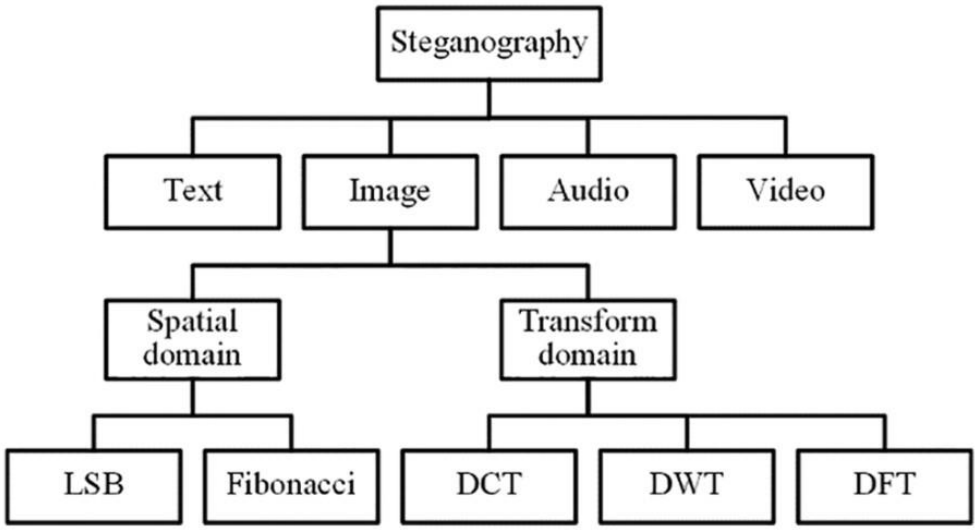

Figure 2 Various type of steganography techniques [12]

1 **Performance Metrics**

An image steganographic technique can be evaluated using three main parameters [4]

i. **Hiding capacity:** The hiding capacity can be referred in two ways, maximum hiding capacity, and bitrate. **The maximum hiding capacity** is the maximum amount of data that can be hidden in the image. It can be represented in bits or bytes or kilobytes. While the **bit-rate** is the maximum number of bits that can be hidden per pixel; it is often termed as bits per pixel (bpp) or bits per byte (bpb). If the hiding capacity is larger, then the steganography technique is better. [7]

ii. **Distortion measure (Visual image quality)**: It is defined by the similarity of the stego-image to the cover image. The stego-images should be undetectable, which means that there should be no detectable distortion in them. The distortion can be measured by using many metrics such as; Mean Square Error (MSE), Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Correlation, Quality Index, Kullback-Leibler Divergence (K-L divergence), Manhattan Distance, and Euclidean Distance [7] [4]

A. Mean Square Error (MSE)

MSE is the most used image quality metric estimator. It is a full reference metric, and the closer the value is to zero, the better. It corresponds to the approximate value of squared error or quadratic loss. MSE can be used to calculate signal fidelity when comparing two signals or images. MSE is simply the average squared difference between the reference and distorted images. Let us consider two images, $\boldsymbol{x(i,j)}$ and $\boldsymbol{y(i,j)}$ of M×N dimensions. The MSE is calculated as [8] [9].

$$\boldsymbol{MSE} = \frac{\mathbf{1}}{\boldsymbol{M \times N}} \sum_{\boldsymbol{i=0}}^{\boldsymbol{M}} \sum_{\boldsymbol{i=0}}^{\boldsymbol{N}} (\boldsymbol{x(i,j)} - \boldsymbol{y(i,j)})^{\mathbf{2}} \quad (\mathbf{1})$$

The higher value of MSE indicates dissimilarity between Cover image and Stego image. The lower the value of MSE, the lower the error. [10] [11]

B. PSNR (Peak Signal to Noise Ratio)

PSNR is used to calculate the ratio between the maximum possible signal power and the power of the distorting noise which affects the quality of its representation. This ratio between two images is computed in decibel form. The PSNR is usually calculated as the logarithm term of decibel scale because of the signals having a very wide dynamic range. This dynamic range varies between the largest and the smallest possible values which are changeable by their quality. The Peak signal-to-noise ratio is the most often used quality assessment metric for determining the quality of lossy image compression codec reconstruction. The signal is the actual data, while the noise is the error caused by compression or distortion. The PSNR approximates human perception of reconstruction

quality when compared to compression codecs. [8]

The PSNR is a measure of stego-image distortion. A higher PSNR value indicates less distortion. A PSNR of more than 40 decibels (dB) is considered excellent. It is acceptable if it is between 30 and 40 dB, but less than 30 dB is not acceptable because the distortion is too high. [7]

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Where R is the maximum value of pixel possible in some its represented as ***(MAX)***

C. Root Mean Square Error (RMSE)

Root Mean Square Error (RMSE) is the standard deviation of the residuals (prediction errors). Residuals are a measure of how far from the regression line data points are; RMSE is a measure of how spread out these residuals are. In other words, it tells you how concentrated the data is around the line of best fit. Root means square error is commonly used in climatology, forecasting, and regression analysis to verify experimental results.

D. Structural Similarity Index Measure (SSIM)

The SSIM index is used for measuring the similarity between two images. The SSIM predicts image quality based on an initial uncompressed or distortion-free image as reference. It tells us how far away an image is from its original reference image more aligned with the human perceptual system. SSIM is designed to improve on traditional methods such as peak signal-to- noise ratio (PSNR) and mean squared error.

iii. **Security:** A steganographic algorithm is said to be secure if different steganalysis algorithms find it difficult to detect the embedded text in the stego-image produced by this approach. Regular-Singular (RS) analysis and Pixel Difference Histogram (PDH) analysis are example of methodologies use for testing the security of a steganographic algorithm.

METHODOLOGY

The methodology used in this performance analysis involved the following steps:

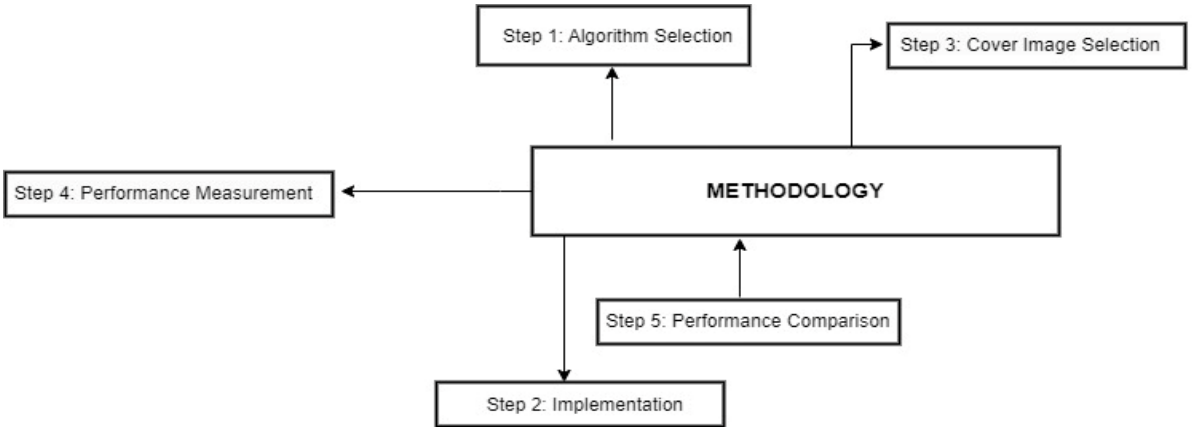

Figure 3 Methodology Flow Chart

i. **Selection of the comparable algorithm:** Selection of the comparable algorithms are based on the common classes of image steganography; spatial and transform domain, most frequently used algorithm were selected from each domain, one from spatial domain and two from transform domain. LSB, DCT, and DWT steganography algorithms are selected. Figure 4, Figure 5 and Figure 6 below shows the DCT algorithm flow chart, DWT Algorithm and LSB Algorithm respectively

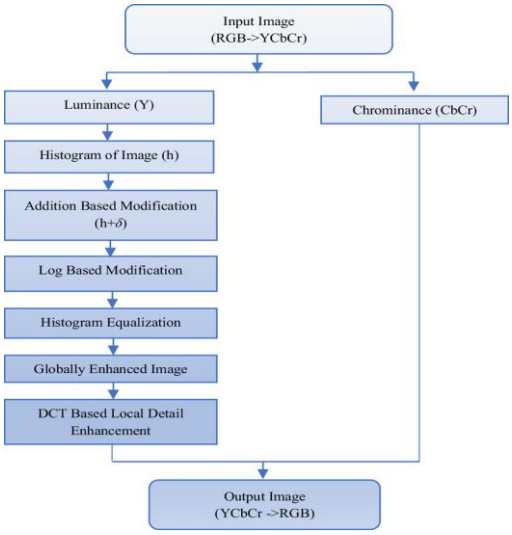

Figure 5 DCT based Algorithm flowchart [13]

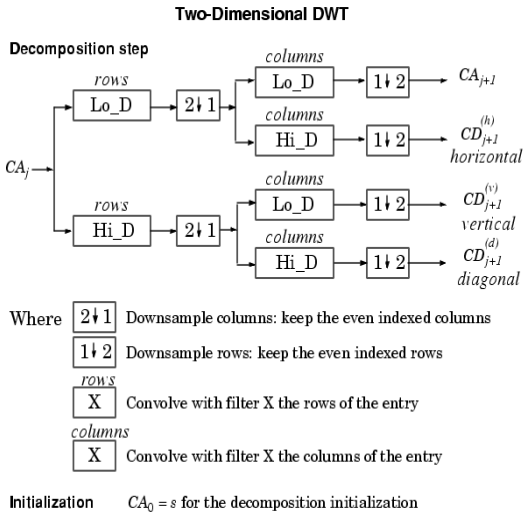

Figure 4 dwt2 algorithm

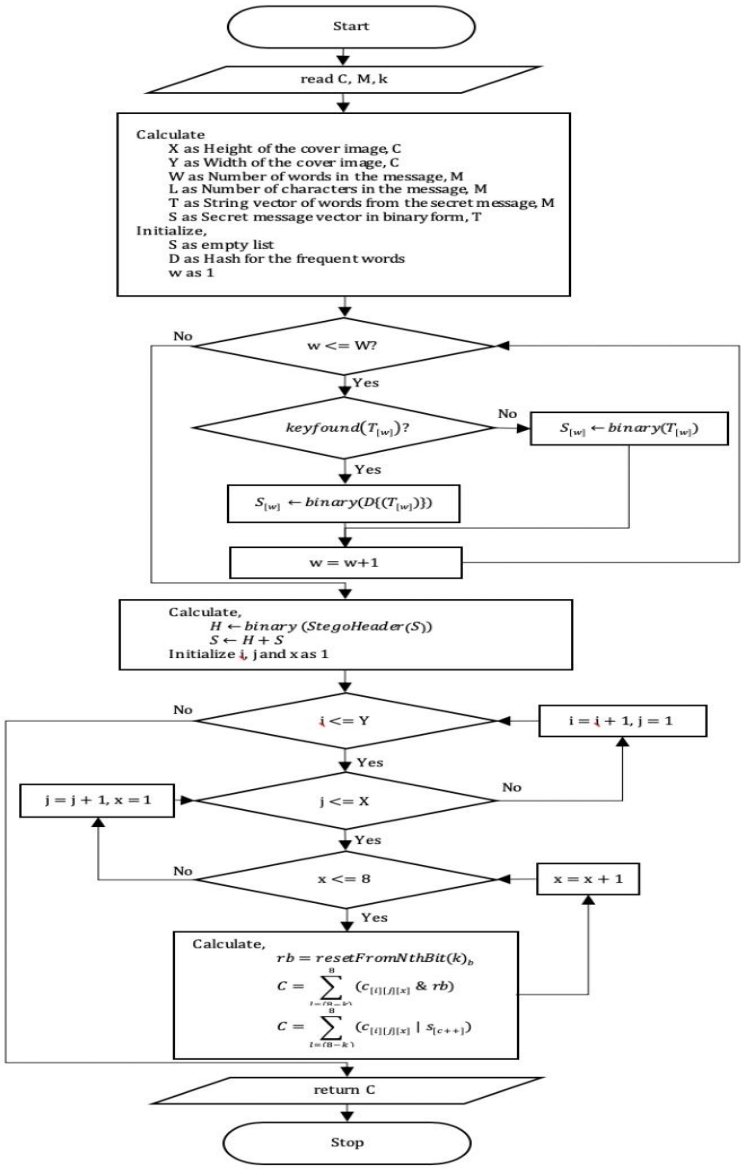

Figure 6 Least Significance Bit Algorithm [14]

ii. **Implementation of the LSB, DCT, and DWT steganography algorithms using Python programming**: One of the main reasons for using Python for the implementation of the LSB, DCT, and DWT steganography algorithms is its wide range of libraries and modules that provide pre-built functions and methods for image processing and digital signal processing, which are essential for steganography algorithms. For instance, Python libraries such as OpenCV, NumPy, SciPy, and Matplotlib are commonly used in image processing and digital signal processing research, which made it a natural choice for the implementation of the steganography algorithms in this study.

Additionally, Python has a large and active community, which makes it easy to find support and resources for troubleshooting and development. Furthermore, Python has an easy to read, understand and write syntax which makes it a great language for teaching and learning. Python's popularity in the academic and research community is also supported by its ability to interface with other languages and tools, such as R and Matlab, which are widely used in data analysis and machine learning. Python is widely accepted, and it is used in many computers vision, machine learning, and data analysis projects. Python's libraries have been tested and proven over time in many research papers, and it is a standard tool for many researchers in the field of image processing and digital signal processing.

iii. **Selection of an appropriate cover image and a secret message to be embedded using each of the algorithms.** Three cover images were selected and used in the research with 200bits character secret message.

(a) *Lena.jpg* (b) Buhari.jpg (c) pepper.jpg

Figure 7: Cover image used for the implementation

The Secret Message used inside the cover picture as shown in figure 7 above is ***"I love my country Nigeria"***

iv. Calculation of the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) for each of the stego images generated using the LSB, DCT, and DWT algorithms.

v. Comparison of the PSNR and MSE values obtained for the stego images to determine the best-performing algorithm in terms of image quality and secret message capacity.

vi. Conclusion and recommendations on the performance of the LSB, DCT, and DWT steganography algorithms based on the results obtained.

RESULT AND DISCUSSION

In this section, we discuss the result of our implemented steganographic algorithms, this program runs under the Microsoft Windows 11 (x64)

operating system. This program is written in Python with the required libraries and module. It is implemented on a HP Laptop equipped with an Intel Core i3-1115G4 whose base frequency is up to 4.1 GHz with Intel® Turbo Boost Technology, 6 MB L3 cache, 2 cores, 4 threads. The RAM capacity is 8 GB and the solid-state drive capacity is 256GB. Below is the summary of the results obtained.

A. Least Significance Bit (LSB)

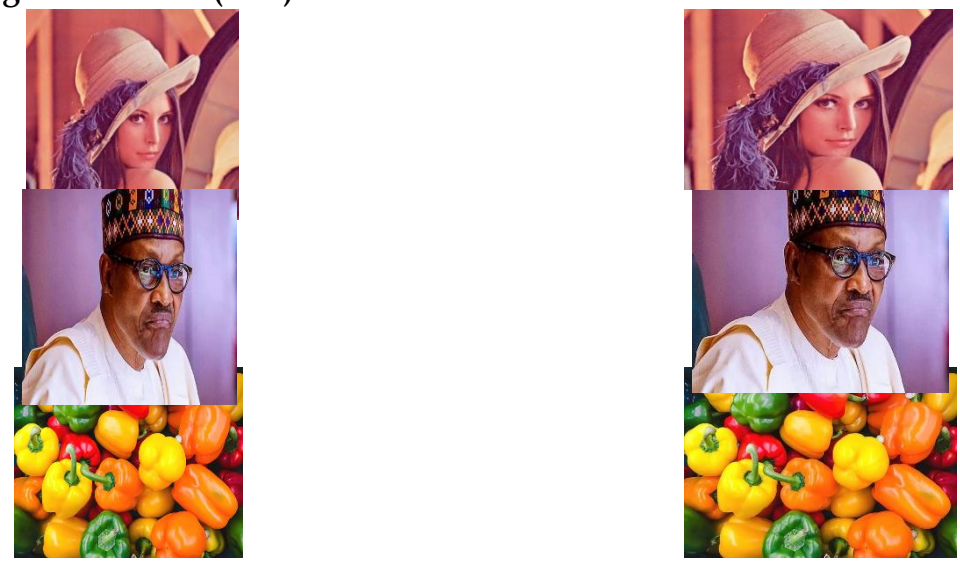

Figure 8 Showing the cover image and the Steg image of LSB algorithm.

Table 1 shows the result of hiding message using LSB. The values of PSNR for algorithm using LSB are 93.6134, 87.2197 and 90.1991 for Lenna, Buhari and Pepper images respectively, and for MSE the value is 0.67. The above figure 8 shows the stego image of the LSB.

Table 1 Summary of the algorithm using LSB

Cover Image	Performance Metrics		
	MSE	PSNR (dB)	File Size(KB)
Lenna.jpg	0.0000028294	93.6137	568
Buhari.jpg	0.00000607	90.29666	598
Pepper.jpg	0.000006211	90.1991	115

B. Discrete Cosine Transform (DCT)

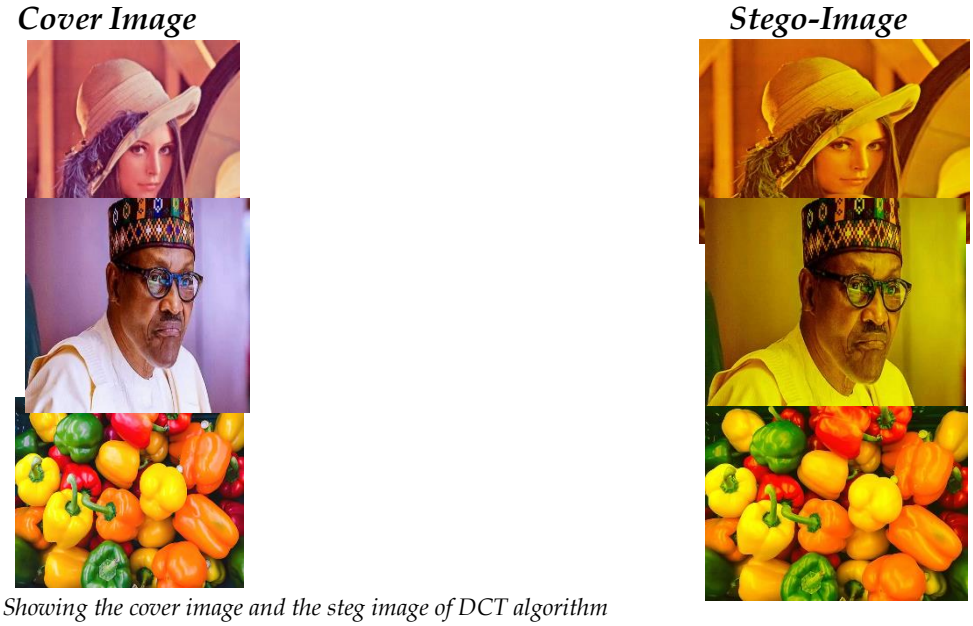

Figure 9 Showing the cover image and the steg image of DCT algorithm

Figure 5 shows the Steg image after hiding the message in the cover image. Table 2 shows the result of hiding message using DCT. The values of PSNR for algorithm using DCT are 93.6134, 87.2197 and 90.1991 for Lenna, Buhari and Pepper images respectively, and for MSE the values are 36.13855, 34.680824 and 33.486024 for the cover image respectively.

Table 2 Summary of Performance of DCT Algorithm

Cover Image	Performance Metrics		
	MSE	PSNR (dB)	File Size (KB)
Lenna.jpg	36.13855	12.3293	93.4
Buhari.jpg	34.680824	8.27093	59.9
Pepper.jpg	33.486024	18.6394027	73.0

C. Discrete Wavelet Transform DWT

Table 3 shows the result of hiding message using DWT. The values of PSNR for algorithm using DWT are 93.6134, 87.2197 and 90.1991 for Lenna, Buhari and Pepper images respectively, and for MSE the value is 0.67.

Table 3 Summary of the performance of DWT Algorithm

Image	**Performance Metrics**		
	MSE	**PSNR (dB)**	**File Size (KB)**
Lenna.jpg	00.13533	14.7472	165
Buhari.jpg	0.1143125	17.66932	98.2
Pepper.jpg	0.0.1436246	16.706756	121

D. Comparative Analysis of LSB, DCT AND DWT

Table 4 Comparative Analysis of LSB, DCT and DWT based on Mean Square Error (MSE)

	LSB	**DCT**	**DWT**
Lenna	0.000028294	36.13855	0.13533
Buhari	0.0000607	34.6808217	0.1143125
Pepper	0.00006211	33.4860242	0.1436246
Average	0.000050368	34.7684653	0.131089

A Mean Square Error (MSE) comparison of LSB, DCT, and DWT provide insights into the image quality of the stego image (the image with the hidden data) produced by each approach. MSE is a common metric for measuring image quality by comparing the differences between the original and reconstructed images. Table 4 summarize the MSE values of each stego-image, the average shows 0.000050368 for LSB, 34.7684653 for DCT and 0.131089 for DWT respectively.

Table 5 Comparative Analysis of LSB, DCT and DWT based on PSNR

	LSB	DCT	DWT
Lenna	93.6137	12.3293	14.7472
Buhari	90.2967	8.27094	17.66932
Pepper	90.1991	18.6394	16.70677
Average	91.36983333	13.07988	16.37443

When comparing the performance of these techniques, it is common to use PSNR (Peak Signal-to-Noise Ratio) as a measure of quality. PSNR is a measure of the similarity between the original and cover images, with higher values indicating better quality. In this result, LSB has the highest PSNR values, followed by DWT and then DCT.

Table 6 Comparative Analysis of LSB, DCT and DWT based on File Size

	LSB	DCT	DWT
Lenna	568KB	165KB	93KB
Buhari	290KB	59.9 KB	98.2KB
Pepper	115KB	73KB	121KB

DCT produce smaller file size followed by DWT then followed by LSB, but LSB has the added advantage of being lossless and can be used for steganography.

Generally, DCT and DWT are considered to be more efficient in terms of compression ratio, compared to LSB. However, LSB has more efficient in terms of MSE and PSNR, these shows LSB has the advantage of being lossless and can be used for steganography, making it more suitable for certain applications.

CONCLUSION

The comparison of the performance of LSB, DCT, and DWT steganography revealed that, while DCT and DWT have a higher compression ratio i.e., have lower file size, LSB has a higher MSE and PSNR, indicating that it is a lossless and more efficient method. Overall, when deciding the steganography approach to use, it is critical to evaluate the application's specific requirements and limits. In this case, we chose LSB over DCT and DWT for best quality, which has been effectively implemented and calculated for various parameters, the results of which have been computed and provided for quality performance from the research effort.

REFERENCES

[1] M. Mohammed Abdul, S. Rossilawati, S. Zarina and H. Mohammad Kamrul, "A Review on Text Steganography Techniques," *Mathematics,* vol. 9, no. 21, 2021.

[2] A. Himanshu, B. Cheshta and D. Sunny, "Comparative study of image steganography techniques," in *Conference: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 2018.

[3] "Edureka Steganography," [Online]. [Accessed 2023].

[4] A. Mostafa A, E. Mourad, S. Ahmed H, A.-S. Ali M., A. Ali, A. K. Monir and I. Costas, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images," *Alexandria Engineering Journal,* vol. 61, no. 12, pp. 10577-10592, 2022.

[5] Y. Liu, S. Liu, Y. Wang and Z. Hongguo, "Video steganography: A review," *Neurocomputing,* vol. 335, no. 28, pp. 238-250, 2019.

[6] J. Chua Teck, W. Chuah Chai, B. A. R. Nurul Hidayah and I. R. B. A. Hamid, "Audio Steganography with Embedded Text," in *IOP Conf. Ser.: Mater. Sci. Eng.*, Melaka, Malaysia, 2017.

[7] P. Anita, S. Aditya Kumar, S. Gandharba and S. K. Raja, "Performance Evaluation Parameters of Image Steganography Techniques," in *International Conference on Research Advances in Integrated Navigation Systems*, India, 2016.

[8] S. Umme, A. Morium and U. Mohammad Shorif, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications,* vol. 7, pp. 8-18, 2019.

[9] D. Tripti and T. Namita, "Different Method Used in Pixel Value Differencing Algorithm," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 18, no. 3, pp. 2278-8727, 2016.

[10] S. Maninder Pal, S. Harmandeep and H. Singh, "Improving Mean Square Error and Peak Signal to Noise Ratio usingXORing Algorithm in Steganography," in *International Conference on Communication, Information and Computing Technology(ICCICT-15)*, 2015.

[11] S. Diksha, B. Indira and B. Manika, "Analysis of Different Image Steganography with Encryption Techniques," *International Research Journal of Engineering and Technology (IRJET),* vol. 7, no. 4, pp. 6179-6184, 2020.

[12] A. S. T. M. T. M. Z. S. M. &. A. A. Rehman, "Data hiding technique in steganography for information security using number theory," *Journal of Information Science, 016555151881630. doi:10.1177/0165551518816303* , vol. 45, no. 6, pp. 767-778, 2018.

[13] A. K. Bhandari, "A logarithmic law based histogram modification scheme for naturalness image contrast enhancement," *ournal of Ambient Intelligence and Humanized Computing,* vol. 11, pp. 1605 - 1627, 2020.

[14] J. Jagan Raj, Kavita and Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in spatial domain of Steganography using character sequence optimization," *IEEE Access,* 2020.