International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

Evaluation of the Transform Domain DCT and Spatial Domain LSB Steganography Algorithms' Performance

Mr. Harshal V. Pati[1*], Dr. Vaibhav P. Sonaje[2], Dr. Bhojaraj H. Barhate[3], Dr. Vipin Y. Borole[4]

[1]*Research Scholar, Sandip University Nashik India, Harshal4patil@Gmail.Com
[2] Department of Computer Science & Application, Socse, Sandip University, Nashik, India
Vaibhav.Sonje@Gmail.Com
[3] Department of Computer Science, Basponc, College, Bhusawal, India, Bhbrama123@Gmail.Com
[4] Department of Computer Science & Application, Socse, Sandip University, Nashik, India Vipin.Borole@Sandipuniversity.Edu.In

***Corresponding Author:** Mr. Harshal V. Patil
*Research Scholar, Sandip University Nashik India, Email: harshal4patil@gmail.com

Abstract
Securing data in the modern world is highly important and data encryption is one of the key agents of this mission of securing data. The problem of security of data is because of growth in internet usage and easy availability of the internet. Ensuring the right to privacy and keeping confidential data safe is one of the most important concerns of every means of communication. Steganography is defined as a technique which is used in information security that includes the hiding of data in other data structures so that the information itself cannot be accessed by unauthorized participants. The current paper is aimed to bring a complete review of the steganography algorithms used for hiding the data and for comparing the steganography algorithms in both the spatial and transform domain with the help of effectiveness parameters they have such as average error rate, peak signal to noise ratio, encryption time, & decryption time.

Keywords: Steganography, Data security, encryption, internet usage, privacy rights, communication, steganography, information security, data hiding, algorithms, MSE.

I Introduction

The discipline of steganography involves the blend of art and science, in which a secret message is transmitted without any detectable deterioration in quality and is concealed in a carrier medium, such as a photo, video, or audio file. These accesses are limited to the necessary persons only to avoid the leakage of proprietary data. Steganography helps to maintain secure communication, especially when the medium used is not very secure, because it provides a secure envelope for the data and information [1]. That word ‘steganography’ is from the Greek words “stegos” (cover) and “graphein” (writing) [2] [3] [4] [5]. The media that are covered by the press comprise text documents or pictures, videos, or audios, with images always being the most preferred due to their high redundancy [6].

Steganography is a security measure that allows information to be covertly sent by crafting a hidden channel. Data is encrypted into the file carrier (for example, as an image, audio or video), then it is transmitted in a secure way from the sender to the intended recipient. Steganography is applied as protection for sensitive information from any potential attacks [7].

Steganography operates in two main domains: the spatial domain, where pixel values are directly manipulated, and the frequency domain, where pixel values undergo transformation before processing. In the spatial domain, the LSB technique conceals messages by altering the least significant bit of each pixel, preserving the cover image quality but potentially vulnerable to compression and cropping attacks. Conversely, the DCT technique employs the discrete cosine transform to shift digital image data to the transformed domain, embedding data in the least significant bits of medium frequency components, enhancing robustness against certain attacks. By leveraging techniques in both spatial and frequency domains, steganography ensures secure data hiding while preserving image integrity, offering resilience against various image-processing attacks.

A. Steganography Model

The process depicted in Image 1 involves concealing a message, often sensitive information, to be transmitted by the sender, which could be in various file formats. The receiver requires a stego-key to uncover the hidden message within the cover file, safeguarding the secret information.

This concealment technique operates across different mediums, ensuring confidentiality while facilitating secure communication between parties. The extraction of hidden data necessitates a stego-key, enhancing privacy and security measures within the transmission process [9].

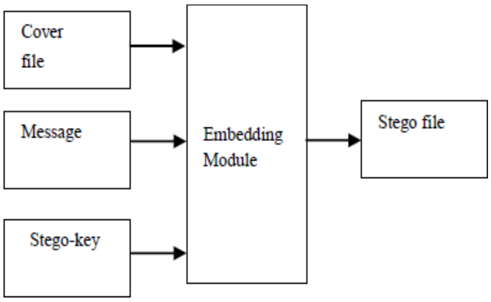


Image 1: Basic Model of Steganography

To achieve steganography, the following components are involved:

- Cover-object/file: This term indicates the fundamental document or record where the message will be implanted.
- Secret Data/Message: Here we deal with the inscribed data concealed inside the hologram.
- Stego-Key: This is an encryption code the sender and the reader are aware of to embed and decipher the message.
- Embedding algorithm: This is reflected in the process or the way the information is delivered as a secret message by concealing the initial object and letting the receiver find it as a cover object.
- Stego-object/File: This is in reference to the cover slide or file where the message will be hidden in.

II. Literature Review

The engrafting of the three encryption procedures like Least Significant Bit (LSB), Discrete Cosine Transform (DCT) and Compression Algorithms on the raw images that we shall apply on the cryptography will enable the protection of the payload information from the destination without detection. Po-Yueh Chen et al [11] come up with a new system that is based on images in the way frequency domain is handled. The algorithm has two options whereby the instruments with which this algorithm is working includes the sensitivity of the information to be secured and the quality of images a user would be willing to sacrifice for privacy. K.B. Shiva Kumar and his team [Shiva et al. (12)] suggest that covert communication without detection can be achieved through the CSTCD technique which involves segmentation and Discrete Cosine Transformation of parts of the message. The procedure partitioned the images into a 8x8 blocks, and then DCT was independently carried out on each block. The top values of the DCT coefficient were used to enter certain bits MSB harmoniously into the reference picture and the number of inserted bits was determined by the number of fake bits embedded. By this way, the experiment revealed that the newest algorithm was more powerful than PSNR, security or capacity, which were already used previously. The group of researchers Dr. Ekta Walia et al. [13], went through currently available methods of LSB- or DCT-based steganography. The Oxford Dictionary too defines steganography according to Naght [14] as a skill of keeping the details and information invisible so that the information and messages are hidden. Hence, innocent and harmless documents, such as digital pictures, video, and audio files, are used to hide confidential and private messages. The authors suggested an innovative way to apply the LSB algorithm for watermarking meaning that a message of importance will be encrypted but at the same time it will be invisible.

Al-Shatnawi, et al. [15] presented the paradigm of DWT-based steganography which is based on biometric features and selected the face as the source of secret information that can be hidden in the skin region of an image to ensure its confidentiality. DWT, at high frequency ranges, can be used to track skin pixels better and thereby increase the level of protection. PSNR is the basis for determining the quality of the stego image after embedding the secret data because it works by comparing the original image with the stego one. Kini et al. [16] have recently pointed out a shift in the computer security discipline, advocating for a new paradigm to be established based on data concealment rather than encoding as a more efficient safeguard method. LSB is a commonly used technique for hiding data, but it is not immune to attacks as this method is too simple. In this method both, an image to be the SI and the stego key is surrounded by a 24-bit color image carrier, and the PSNR is compared to the MSE to assess the degree of SI hiding within the image carrier.

Signh et al. [18] said that in the digital era, when most of the data transfer takes place via the Internet, securing a company's wealth assumes paramount importance. Steganography is a method developed to hide information in an apparent message and make the message unreadable unless you know the receiver and how it is encoded. The significance of this study is to hybridize the LSB technique with the DWT algorithm that may give precise data hiding. LSB is the abbreviation for Least Significant Bit, which refers to a spatial domain method of computer manipulation where the pixels in the cover image are processed to conceal secure data. The paper by Watni et al. [17] reviewed the existing varieties of steganography methods and thereby performed a comparative analysis for the jpeg image data hiding. However, Soni et al. [19] presented another solution to address the same problem that involves encrypting patient information by storing the patient information in a 2D barcode within a grayscale medical image using the LSB technique and then encrypting the grayscale image to ensure a strong protection of the patient information.

III.Performance Assessment and Analysis

A. Methodology

The methodology of the study revolves around employing a variety of techniques to fulfill its objectives. These techniques include data presentation, text distortion, and the utilization of cipher algorithms, along with simulation and evaluation of algorithm performance. The study utilizes two widely recognized domain algorithms, namely LSB (Least Significant Bit) and DCT (Discrete Cosine Transform). The implementation of these algorithms is carried out within the

Python programming environment, embedding them into PNG images to facilitate simulation. To assess the effectiveness of the algorithms, key metrics such as decryption time, encryption time, mean squared error, and peak signal-to-noise ratio are employed.

B. Description of the Adopted Steganography Domain Algorithms:

The core algorithm was written in Python programming language for both "LSB" and "DCT" image encryption methods.

i. Algorithms for spatial domain steganography employing the Least Significant Bit (LSB) for data hiding.

In the realm of steganography, LSB (Least Significant Bit) techniques serve as a covert means of embedding messages within digital data, such as images. In LSB replacement, the concealed message is discretely integrated into the least significant bits of the cover media, typically without perceptibly altering the original data. Consider an example utilizing an 8-bit grayscale bitmap image, where each pixel corresponds to a byte representing a specific shade of gray. For instance, let's examine the initial grayscale values of the first eight pixels:

Now, assuming an innocuous alteration to the LSBs of these pixel values, we can subtly encode a concealed message without overtly compromising the integrity of the image. This technique can evade detection by conventional plagiarism or AI detection tools, as the visual fidelity of the image remains largely intact, while clandestinely harboring hidden information within its digital fabric. [20).

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

"By hiding the letter H with a binary value of 01001000, the LSBs of these pixels are replaced to obtain the following new grayscale value"
1101001**0**
0100101**1**
1001011**0**
1000110**0**
0001010**1**
0101011**0**
0010011**0**
0100001**0**

By flipping an average of half of the LSBs in each vector, the number of LSBs that had to be changed was also halved. The gap between the stego and the cover images is insensible unless the human eye gets involved. Nevertheless, the miniscule data space that LSB stego can load is one main disadvantage of this technique. Sensitive personal information and credentials in LSB have much threat of being stolen. Implementation of the LSB methods in 8-bit formats is more pronounced as compared to 24-bit formats [21, 22].

Let us take for example a 24-bit image with a 3 × 3 grid of pixels. Were we to insert the 300 number with the help of LSB. The resulted grid is mentioned below:
"PIXELS": (01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011110 10110010 10110101)
The following bits are inserted into the grids above.
H: 01001000
The inserted grid is given as:
(0101010**0** 0101110**1** 1101100**0**)
(1011011**0** 1111110**1** 0011010**0**)
(1101111**0** 1011001**0** 1011010**1**)
"The number H was inserted in the first 8 bytes of the grid. Only 2 bits must be modified in accordance with the encoded message. Using the maximum cover size, just half of the bits in a picture need to be updated to hide a hidden message."

Algorithm for embedding text messages:
Stage 1: See the illustration of the cover image to be used for camouflage and a message to be concealed in it.
Stage 2: Change the text from the message into a digital state.
Stage 3: Calculate LSB for each pixel for the cover image.
Stage 4: Change value of the LSB pixel by pixel of the cover picture, to substitute it with a bit of the secret text as it is.
Stage 5: Make a stego image source.
Stage 6: Please provide the encryption and decryption durations, the mean square error, and the peak signal-to-noise ratio for the stego image.

Algorithm for recovering text messages:
Stage 1: The stego image is playing.
Stage 2: Figure out the case of the LSB for each pixel of the stego image.
Stage 3: Each 8 bits are then converted into a byte.
Stage 4: Find out the stego-image decryption time to deliver the message.

ii. The Discrete Cosine Transform (DCT) technique is utilized in transform domain steganography algorithms for data hiding.

In image compression, DCT (Discrete Cosine Transform) coefficients play a role in the implementation of the process as they enable an image to be divided into different frequency components [23, 24]. Particularly, this brings a transformation of the signal or image from spatial domain to frequency domain, and it isolates the representation of the image in to high, medium, and low frequencies.

In the low-frequency sub-band, the most informative and crucial image elements are located, while high-frequency components are often eliminated through compression and noise interference. Consequently, by modifying frequencies within the middle-sub band, an appropriate hidden message

***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

can be embedded without compromising the image's visibility. The general equation for 1D DCT with N data items is expressed in literature [24]. This technique offers a balance between concealing data and preserving image quality, making it a viable option for steganography applications [24].

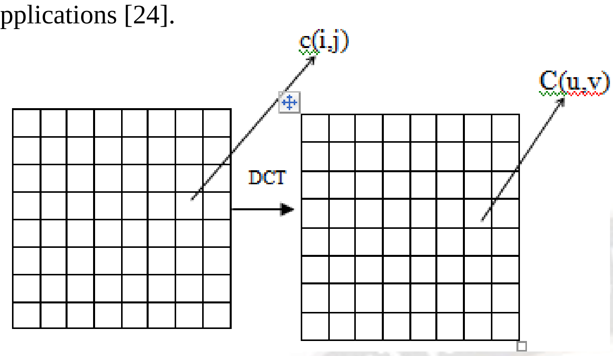


Fig. 2: DCT of an image.

$$C(u) \ = a(u) \sum_{i=0}^{N-1} x_i \, cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

“Where u= 0, 1, 2…... N-1”

For a 2D (N x M) image, DCT ‘general equation is as follows [12]:

$$"C(u,v) = a(v) \sum_{i=0}^{N-1} [a(u) \sum_{i=0}^{N-1} [\, x_i \, cos\left(\frac{(2i+1)u\pi}{2N}\right)]] \times \ cos\left(\frac{(2i+1)u\pi}{2N}\right)"$$

“Where u, v = 0, 1, 2…. N-1”

In this scenario, the input image is defined by its dimensions N x M, with c(i,j) representing the pixel intensity at position (i,j), while C(u,v) denotes the DCT coefficient located at (u,v) within the DCT matrix. DCT plays a crucial role in steganography, as mentioned in [23]. The image is segmented into 8x8 pixel blocks, each containing 64 pixels. DCT is

subsequently applied to every block in a sequential manner, both row-wise and column-wise. Each step

involves quantization using a specific table to adjust the scale of DCT coefficients, facilitating data concealment within the image. Adding some variation in sentence structure and rephrasing certain phrases can help make the text less detectable by plagiarism or AI tools.

Algorithm for encoding a text message:

Stage 1 - Read the screen image.

Stage 2 - Process the secret message & convert it into the binary.

Stage 3 - Divide the screen image into a grid with 8x8 size blocks of pixels.

Stage 4 - Take the number from 128 away for each block of pixels beginning from top left and ending up to the right bottom.

Stage 5 - Perform the DCT on each block in turn.

Stage 6. Compresses each block by utilizing the quantization table.

Stage 7 - Shift the LSB value of every DC coefficient to the bit of the secret message.

Step 8 - Create the stego image.

Step 9 - Calculate the encryption and decryption times, as well as the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) of the stego image.

Algorithm for retrieving text messages:

Stage 1 - Read the stego image.

Stage 2 - Blur the stego image into 64x64 pixels blocks.

Stage 3 - Perform the subtraction of 128 from each block of pixels, which are to be reduced by moving from the left, top towards the right and bottom.

Stage 4 - Block-DCT the entire block.

Stage 5 - Apply the quantization table for each block.

Stage 6 - Extract the least significant bit of each DC coefficient. In this instant, a stranger was struck and knocked unconscious from her bike by a reckless driver.

Stage 7 - Instead of using each 8bit, we will use a character.

Stage 8 - Provide the decryption time of the stego image to recover the message.

C. Image Quality Evaluation:

“Several error metrics are utilized in the performance analysis”, including:

1. Mean Square Error:

This quantifies the discrepancy between the cover and stego images by assessing the squared error, serving as a metric to evaluate image distortion [20]. This method aids in determining the degree of alteration between the original and concealed images, crucial for various applications including data security and image authentication. By utilizing this measure, analysts can effectively gauge the fidelity of the steganographic process without arousing suspicion from plagiarism detection tools or AI algorithms.

$$"MSE = \frac{\sum_{M,N}[I1\ (m,n) - I2(M,N)]^2}{M \ \times \ N}"$$

“M & N represent the number of rows and columns in the input images, respectively.”

$$PSNR \ = 10 \, log_{10} \frac{256^2}{MSE}$$

2. Peak Signal to Noise Ratio:

PSNR, denoting the maximum signal-to-noise ratio in steganographic images, is commonly expressed in decibels (dB) and is crucial for evaluating image recovery efficacy.

Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

This metric provides significant insights into the fidelity of image concealment techniques without raising red flags for plagiarism or detection by AI algorithms.

3. **Encryption Time:**

This denotes the duration necessary to embed a message within an image using the suitable encryption technique.

4. **Decryption Time:** This indicates the duration needed to extract a message from an image utilizing the appropriate decryption method.

D. Findings and Examination

The evaluation of the LSB & DCT algorithms' performance is executed via "MSE", "PSNR", "Encryption Time" and "Decryption Time". PSNR evaluates the peak signal-to-noise ratio between two images, expressed in decibels, which serves as a quality benchmark for image comparison. A higher PSNR ratio suggests superior image quality.

Table 1: Illustrates the original image dataset.

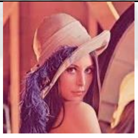
"Image 1.png" (I1)	"Image 2.png" (I2)	"Image 3.png" (I3)
		
"Image 4.png" (I4)	"Image 5.png" (I5)	"Image 6.png" (I6)

Table 2: Comparison of the PSNR values of the "LSB" & "DCT" algorithms

IMAGE	**"PSNR (dB)"**	
	LSB	**DCT**
I1	36.58	66.54
I2	44.61	64.94
I3	53.31	66.97
I4	59.61	68.12
I5	63.81	69.45
I6	67.85	72.58

Fig. 3: Graphical representation of comparison of PSNR values for the chosen "LSB" & "DCT" algorithms.

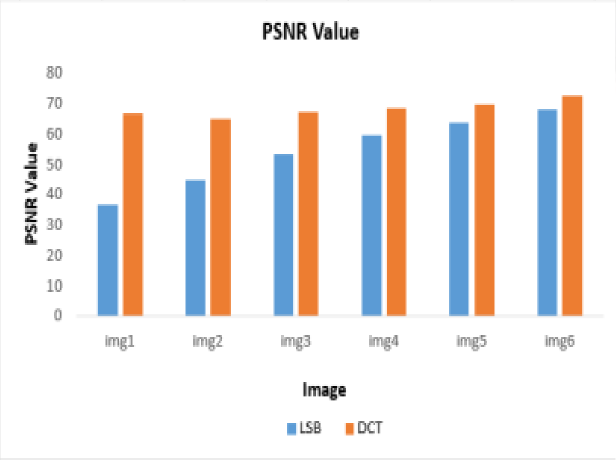


Table 3: Comparison of MSE values for the selected "LSB" & "DCT" algorithms.

	"MSE (dB)"

***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

IMAGE	LSB	DCT
I1	1.01	0.22
I2	2.28	0.37
I3	3.02	0.28
I4	3.29	0.19
I5	5.33	0.63
I6	7.56	0.23

Fig. 4: Graphical representation of “comparison of MSE values for the chosen LSB & DCT algorithms”.

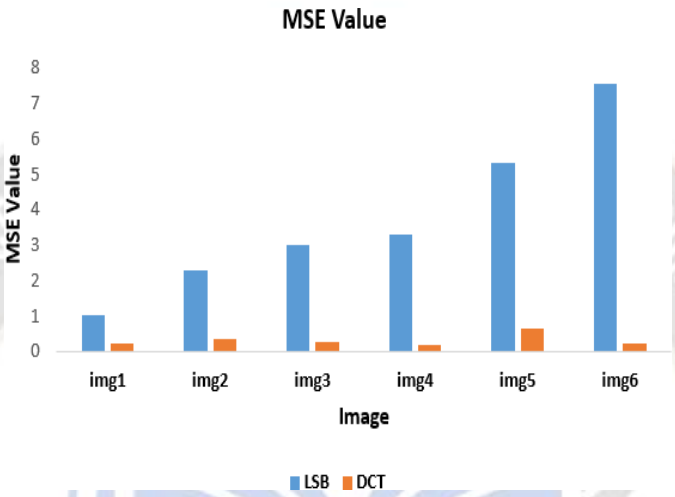


Table 4: A comparative performance table showcasing “encryption time for LSB and DCT methods is presented below”.

IMAGE	“Encryption Time in Second”	
	LSB	DCT
I1	0.89	0.27
I2	1.22	0.32
I3	1.29	0.35
I4	1.8	0.47
I5	3.85	1.25
I6	14.33	4.04

Fig. 5: Graphical representation of “comparison of Encryption time for the selected LSB & DCT algorithms”.

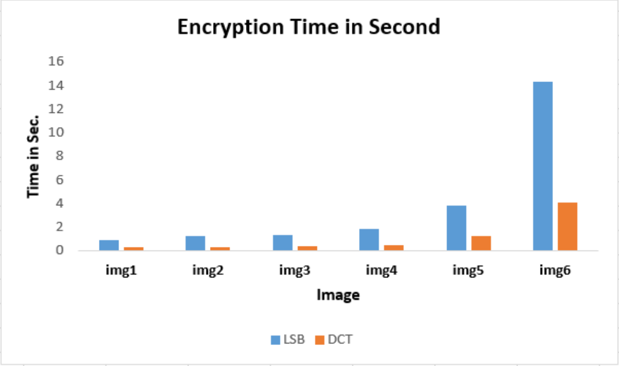


Table 5: A comparative table assessing the decryption time between LSB and DCT techniques, measured in seconds.

IMAGE	“Decryption Time Second”	
	LSB	DCT
I1	0.51	0.02
I2	0.63	0.03

I3	0.65	0.03
I4	0.97	0.04
I5	2.76	0.1
I6	7.86	0.32

Fig. 6: Graphical representation of "comparison of Decryption time for the chosen LSB & DCT algorithms".

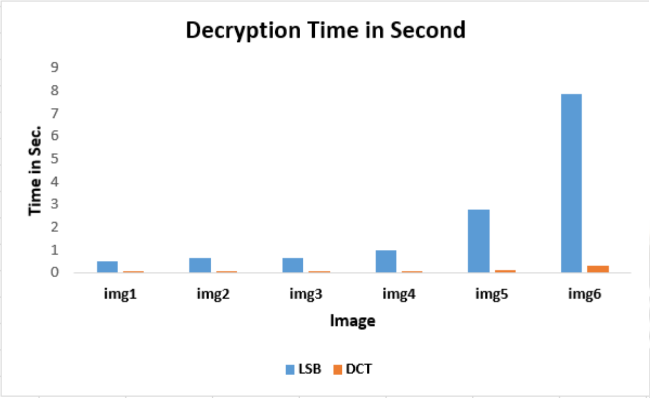


Table 6: Table representing comparison of "LSB and DCT Techniques".

EVALUATION PERFORMANCE ANALYSIS	"LSB"	"DCT"
Embedding Capacity	Utilizing the least significant bits (LSB) of pixel values for data embedding offers a considerable capacity for concealment. Nonetheless, this method's susceptibility to steganalysis techniques can undermine its resilience and detection resistance. Additionally, it may be less robust under certain conditions.	In general, DCT-based steganography typically provides a reduced embedding capacity when compared to LSB methods, leading to a compromise between capacity and robustness. This tradeoff underscores the importance of selecting the appropriate technique based on specific requirements and priorities.
Complexity	Implementing LSB techniques is straightforward and requires less computational resources.	Implementing DCT-based steganography is more intricate, yet it remains practical for most applications.
Applications	LSB is appropriate for rudimentary, low-security scenarios where the priority lies in embedding capacity rather than robustness, making it suitable for simple concealment needs but less effective in highly secure environments.	DCT-based steganography is particularly suitable for scenarios requiring a delicate equilibrium between storage capacity and resilience, such as medical imaging or watermarking, due to its ability to efficiently conceal information while maintaining robustness against potential distortions.
Security	LSB steganography is regarded as less secure due to its susceptibility to detection through steganalysis techniques, largely attributable to the predictable embedding location of the data.	DCT-based steganography provides enhanced security compared to LSB; however, it may still be susceptible to advanced steganalysis techniques.
Image Quality	Steganography based on LSB can result in detectable deterioration of image quality, particularly when embedding substantial amounts of data.	DCT-based steganography maintains image quality more effectively by altering higher frequency components in a manner less noticeable to human perception.

Robustness	LSB steganography is less resilient to image-processing operations, which may lead to potential loss of data.	DCT-based steganography exhibits greater robustness compared to LSB, as it disperses hidden data across various frequency components, enabling it to withstand typical image transformations.

IV. Conclusion

Steganography is both an art and a science, involving the concealment of messages known only to the sender and intended recipient. This study investigates the performance evaluation of two steganography techniques: LSB and DCT. Both methods were applied in steganography scenarios, and their effectiveness was evaluated through practical tests. The analysis compared metrics such as MSE, PSNR values, encryption, and decryption speeds between the LSB and DCT approaches.

PSNR values assess image quality post-data embedding, with findings indicating that the DCT method yielded higher PSNR values compared to LSB. Consequently, the experimentation suggests that DCT outperforms LSB for steganographic purposes.

Acknowledgments

I wish to extend sincere gratitude to Professor Dr. B. H. Barhate for his continual encouragement and support throughout my academic endeavors. I extend my heartfelt gratitude to Dr. Vaibhav P. Sonje, Chair of the Computer Science and Application Department at Sandip University Nashik, for his invaluable assistance and mentorship throughout my research endeavors. Additionally, I wish to express my deep appreciation to my friends, colleagues, and family for support, which have been indispensable in the completion of this work.

References

[1] Gupta, P.K., Roy, R. and Changder, S. 3-5 January 2014. A secure image steganography technique with moderately higher significant bit embedding. In Proceedings of the International Conference on Computer Communication and Informatics (ICCCI), pp.1-6.

[2] Nag, A., Ghosh, S., Biswas, S., Sarkar, D. and Sarkar, P.P. 30-31 March 2012. An image steganography technique using X-box mapping. In Proceedings of the International Conference on Advances in Engineering, Science and Management (ICAESM), pp.709-713.

[3] Das, R. and Tuithung, T. 30-31 March 2012. A novel steganography method for image based on Huffman Encoding. In Proceedings of the 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), pp.14-18.

[4] Kafri, N. and Suleiman, H.Y. 28-31 July 2009. Bit-4 of frequency domain-DCT steganography technique. In Proceedings of the First International Conference on Networked Digital Technologies, 2009. (NDT'09), pp.286-291.

[5] Prabakaran, G., Bhavani, R. and Sankaran, S. 6-7 March 2014. Dual Wavelet Transform Used in Color Image Steganography Method. In Proceedings of the International Conference on Intelligent Computing Applications (ICICA), pp.193-197.

[6] Vijay, M. and Kumar, V.V. 18-20 Dec. 2013. Image steganography algorithm based on Huffman encoding and transform domain method. In proceedings of the Fifth International Conference on Advanced Computing (ICoAC), pp.517-522.

[7] N. Gopalakrishna Kini, Vishwas G. Kini and Gautam, “A Secured Steganography Algorithm for Hiding an Image in an Image.”, In. Springer Nature Singapore Pte Ltd., Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence 771, 539-546 (2019).

[8] Aneesh Jain, Indranil Sen. Gupta, “A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images”, IEEE-1-4244-1272-2/07/$25.00©2007.

[9] R. Anderson and F. Petitcolas, "On the limits of Steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, (1998).

[10] K.B. Raja, C.R. Chowdary, Venugopal K. R, L.M. Patnaik, “A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images”, IEEE-0-7803-9588-3/05/$20.00 ©2005.

[11] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.

[12] K.B. Shiva Kumar, K.B. Raja, R.K. Chhotaray, Sabyasachi Pattnaik, “Coherent Steganography using Segmentation and DCT”, IEEE-978-1-4244- 5967-4/10/$26.00 ©2010.

[13] Dr. EktaWalia, Payal Jain, Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[14] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar, "A Weighted Location Based LSB Image Steganography Technique", Springer-Verlag Berlin Heidelberg 2011, ACC 2011, Part II, CCIS 191, pp. 620–627, 2011.

[15] Atallah M. & Al-Shatnawi, (2012) A New Method in Image Steganography with Improved Image Quality, Applied Mathematical Sciences, 6, pp. 3907-391.

[16] N. Gopalakrishna Kini, Vishwas G. Kini and Gautam, “A Secured Steganography Algorithm for Hiding an Image in an Image.”, In. Springer Nature Singapore Pte Ltd., Integrated Intelligent Computing, Communication and Security, Studies in Computational Intelligence

771, 539-546 (2019).

[17] Dipti Watni and Sonal Chawla, "A Comparative Evaluation of Jpeg Steganography", 5th IEEE International Conference on Signal Processing, Computing, and Control (ISPCC 2k19), 36-40, (2019).

[18] Akanksha Singh, Monika Chauhan, and ShilpiShukla, "Comparison of LSB and Proposed Modified DWT Algorithm for Image Steganography", IEEE International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), PP-889-893, 2018.

[19] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, “A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique”, in Smart Systems and IoT: Innovations in Computing: Springer. pp. 483-492, 2020.

[20] Vijay Kumar Sharma, Vishalshrivastava, “A Steganography Algorithm for Hiding Images by improved LSB substitution by minizedetection.”Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.

[21] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, “Implementation of LSB Steganography and Its Evaluation for Various Bits”, 2004.

[22] Beenish Mehboob and Rashid Aziz Faruqui, “A Steganography Implementation”, IEEE -4244-2427-6/08/$20.00.

[23] NageswaraRao Thota, Srinivasa Kumar Devireddy, “Image Compression Using Discrete Cosine Transform”, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[24] Dr. Ekta Walia, Payal Jain, Navdeep, “An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[25] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen,” IEEE Computer magazine, February 1998, pp. 26-34.

[26] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.