AN INNOVATIVE METHOD TO ENHANCE THE DISTORTION MEASURE OF IMAGE STEGANOGRAPHY BY DISCRETE COSINE TRANSFORMATION ALGORITHM (DCT) BY COMPARING WITH OPENCV ALGORITHM TO ACHIEVE PEAK SIGNAL TO NOISE RATIO.

Aarthi B L[1], Dr. K. Malathi[2*]

Article History: **Received:** 12.12.2022 **Revised:** 29.01.2023 **Accepted:** 15.03.2023

Abstract

Aim: To enhance the distortion measure of encoded images in the process of Image steganography using Discrete Cosine Transformation(DCT) by comparison with the OpenCV Algorithm.
Methods and Materials: The two groups are OpenCV (N=10) and Discrete Cosine Transformation (N=10). G-power is calculated for two different groups, alpha (0.05), power (80%).
Results: The distortion is measured based on Peak Signal to Noise Ratio(PSNR) value where the Discrete Cosine Transformation has the Peak Signal to Noise Ratio(PSNR) value as 52. The two algorithms Discrete Cosine Transformation and OpenCV are statistically satisfied with the independent sample T-Test (α = .001) value ($p<0.05$) with a confidence level of 95%.
Conclusion: Compared to OpenCV Algorithm, the distortion measure seems to be better in Discrete Cosine Transformation.

Keywords: Innovative Method, OpenCV, Image Steganography, Distortion measure, Data, Algorithm**,** Discrete Cosine Transformation(DCT), PSNR, Steganography.

[1]Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, 602105.
[2*]Project Guide, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, 602105.

1. Introduction

Image Steganography is the process of binding information that is text into a cover image. It is a type of art where invisible communication will take place (Pradhan et al. 2016). The information hidden in the images is not visible to human eyes. There are four types, Audio Steganography, Video Steganography, Text Steganography, and Image Steganography. In this paper, the major discussion is based on Image Steganography. There are two types of techniques in Image steganography, Spatial Domain Techniques and Transform Domain techniques. Some of the Spatial domain Techniques are LSB substitution, pixel value differencing (PVD), etc, and Transform Domain Techniques are DCT, DWT, etc. Here, the paper will discuss and compare two methods that are Discrete Cosine Transformation and OpenCV algorithms. Image Steganography allows two parties to communicate secretly and covertly. Some of the reasons why data hiding is important are, personal and private data, sensitive data, confidential data, and trade secrets, to avoid misuse of data, unintentional damage of data, human error and accidental deletion of data, monetary and blackmail purposes and to hide traces of crime (Хорев and Сергеев 2020). Moreover, there are applications like confidential communication and secret data storage (Fridrich 2010). Also, it allows for copyright protection on digital files using the message as a digital watermark. Protection of data alteration, access control system for digital content distribution, and media database systems (Sharma and Madhusudan 2015).

Totally more than 50 related articles were published in IEEE and more than 30 plus related articles are published in Google Scholar like ResearchGate and Sciencedirect. Some of the most cited articles and their findings are, (Elharrouss, Almaadeed, and Al-Maadeed 2020) an author who proposed an innovative method called image Steganography that is implemented using K-Least Significant Bit. The last three Significant Bits are used to embed a text message into a cover image. A method to improve image quality is added to the process after decoding the messaging from the image. As a result, the Peak Signal to Noise Ratio value is very low, that is 33. (Arun and Murugan 2017) the writer proposed a design of Image Steganography using Least Significant Bit XOR Substitution method for improving security. Here, a random 8-bit secret key that initially XOR with RGB colors is used. Indeed, the storage capacity in the image for data sharing is also improved. (Jaradat, Taqieddin, and Mowafi 2021) the paper implemented Image Steganography using chaotic maps and the PSO algorithm aiming at finding the best pixel location to embed the message. Here, the image is divided into 4 blocks. In this paper, the final result has improved the distortion to a minimal value. Also, the Peak Signal to Noise Ratio value is improved to 64. (Swain 2014) the author implemented Image steganography using nine-pixel differencing and modified Least Significant Bit technique. Here, the image is divided into 3*3 non-overlapping blocks. The PSNR results as an average value of 42. Among all the papers, in my opinion, the best technique is implementing image steganography using chaotic maps and PSO algorithm as it results in a very high PSNR value, which leads to minimizing distortion.Our team has extensive knowledge and research experience that has translated into high quality publications (Mohan et al. 2022; Vivek et al. 2022; Sathish et al. 2022; Kotteeswaran et al. 2022; Yaashikaa et al. 2022; Saravanan et al. 2022; Jayabal et al. 2022; Krishnan et al. 2022; Jayakodi et al. 2022; Mohan et al. 2022)

Communicating through a secret path must always be confidential with good efficiency. The problem that has to be improved is minimal distortion, high quality, and embedding capacity of an image. Now, the growing trend in this area has motivated us to do this project. Steganography is different from Cryptography where the aim is to hide the data wherein in Cryptography the data was converted to encrypted form. The advantages of using Steganography over Cryptography are that the hidden data is hard to detect and it is not susceptible to attacks such as rotation and translation. The value of the Peak Signal to Noise Ratio value must be high to improve the image quality using distortion measure as a parameter. The study aims to improve distortion measures using the parameters Peak Signal to Noise Ratio and Mean Square Error(MSE).

2. Methods and Materials

The innovative work is done in the Object Oriented Analysis and Design laboratory, Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS. There were two groups. The first group is the Discrete Cosine Transformation algorithm(N=10) and the second group is the OpenCV algorithm(N=10). Among the two groups, group 1 is the innovative model which is also an innovative method, and group 2 is an existing model. The results were calculated (Kang 2021) using G* power software and the minimum power of the analysis is fixed as 0.8 and the

maximum accepted error is fixed as 0.5 with a threshold value of 0.05% and the Confidence Interval is 95%. In this analysis, since the major parameter is the number of pixels of each image, different images are used to get the different Peak Signal to Noise Ratio values. Also, different formats of images like png, jpg, jpeg, etc can be used with different resolutions to check for a variation in image capacity, distortion, and image quality using Peak Signal to Noise Ratio value.

OpenCV

(Singh 2019) OpenCV algorithm is the easiest and simplest method to perform Image Steganography. This method gives a low Peak Signal to Noise Ratio value when compared to Discrete Cosine Transformation and Least Significant Bit too. Here, the existing method uses encrypted data to include other data, which significantly impairs the visual representation of the image. The hidden message is transmitted by increasing the bandwidth of the original message or by manipulating the file format. Also, using OpenCV the Image Steganography is difficult to detect.

Pseudo Code for OpenCV

The algorithm steps for OpenCV are:

1. Here, the Tkinter dialog box is used.
2. Use the Tkinter file dialog library to open the file using the dialog box.
3. Obtain the image of the path.
4. Load the image into the GUI using the thumbnail function from Tkinter.
5. Load the image as a NumPy array for efficient computation and change the type of unsigned int.
6. Break the image into character level.
7. Represent character in ASCII.
8. Encode.
9. Then, Decode it.
10. Join all the bits to form letters.
11. Also, Join all the letters to form messages.
12. Then, along with the encrypted image, print the Peak Signal to Noise Ratio value after calculating it.

Discrete Cosine Transformation(DCT)

It helps to separate the image into parts (or spectral sub-bands) of differing importance (to the image's visual quality). This innovative method especially supports JPEG image format. Discrete Cosine Transformation is similar to Discrete Fourier Transform. It transforms a signal or image from the spatial domain to the frequency domain. Here, it can also convert the images into high, middle, and low-frequency components (Sheidaee and Farzinvash 2017). The secret messages are embedded by modifying the coefficients of the middle-frequency sub-band; this method is followed so that the visibility of the image will not be affected. The message is not embedded in the low-frequency sub-band as the most important visual parts of the image are present there and in the high-frequency sub-band, the high-frequency components will be removed through compression and noise attacks. Each block is compressed through a quantization table to scale the Discrete Cosine Transformation coefficients and the message is embedded in DCT coefficients. Fig. 1, represents the flowchart of the Discrete Cosine Transformation Algorithm.

Pseudocode for DCT

The basic operations of the Discrete Cosine Transformation are:

Algorithm to embed text messages:

1. Read the cover image.
2. Read the secret messages and convert them into binary.
3. The cover image is broken into 8×8 blocks of pixels.
4. Working from left to right, top to bottom subtracts 128 in each block of pixels.
5. DCT is applied to each block.
6. Each block is compressed through a quantization table.
7. Calculate the LSB of each DC coefficient and replace it with each bit of secret message.
8. Write a stego image.
9. Calculate the Mean square Error (MSE), Peak Signal to Noise Ratio (PSNR) of the stego image.

Algorithm to retrieve text messages

1. Read the stego image.
2. Stego image is broken into 8×8 blocks of pixels.
3. Working from left to right, top to bottom subtracts 128 in each block of pixels.
4. Discrete Cosine Transformation is applied to each block.
5. Each block is compressed through a quantization table.
6. Calculate the LSB of each DC coefficient.
7. Retrieve and convert each 8 bit into character.

For comparing both the models, different images like a set of 10 images for each algorithm are used for calculating MSE, PSNR values. Finally, choose the algorithm which has higher values of PSNR and lower error of MSE. The Peak Signal to Noise Ratio value is inversely proportional to the Mean Square Error. The system configuration is used for the algorithm to run in a 64-bit Operating System, 4GB RAM PC, SPSS tool, Google Colab, Python

3.8, SPSS software, Windows 10, and Microsoft Office for software specification. To estimate which algorithm gives the best performance the paper compares Peak Signal to Noise Ratio and Mean Square Error values. This also tells us the image quality with the capacity that can be embedded in the image.

3. Results

The change in images and their formats will result in a change in Peak Signal to Noise Ratio value. From Table 1, the Peak Signal to Noise Ratio values have been calculated for the data collection of sample size(N=10). From the results, the paper concludes that the Discrete Cosine Transformation has More Peak Signal to Noise Ratio value compared to the OpenCV algorithm. Moreover, this could also be concluded as Discrete Cosine Transformation has the higher image quality and embedding capacity as it has got better values than OpenCV. Also, the distortion is minimal in the Discrete Cosine Transformation algorithm. Table 1 represents the data collection from the N=10 sample of images to gain Peak Signal to Noise Ratio and reduce Mean Square Root for increase(%) of image quality and embedding capacity(%). ("Peak Signal-to-Noise Ratio" n.d.) here, the formula is used to calculate Mean Square Root which gives us a lead to calculate the Peak Signal to Noise Ratio value. Also, there is a formula to calculate PSNR from MSE. The lower the Mean Square Error, the higher the Peak Signal to Noise Ratio value will result. The IBM SPSS version 21 statistical software is used for the study. The independent variables are the pixel values and the dependent variables are PSNR, MSE, image quality, and embedding capacity in the study, Image Steganography. In SPSS, the data is collected of sample size N=10 for both OpenCV and Discrete Cosine Transformation algorithm. GroupID is given as a grouping variable and PSNR is given as a testing variable. GroupID is given as 1 for OpenCV and 2 for Discrete Cosine Transformation. Group Statistics is applied for the Statistical Package for the Social Sciences (SPSS) collected data and shown in Table 2. By performing the statistical analysis group statistics represents the comparison of the PSNR of OpenCV and Discrete Cosine Transformation. The Discrete Cosine Transformation has the highest value of PSNR as 53.1 and the lowest is 51 in Table 2. This concludes that image quality and embedding capacity is better in the Discrete Cosine Transaction algorithm when compared to the OpenCV algorithm. Figure 2, represents the comparison chart for the Discrete Cosine Transformation and OpenCV algorithm using Peak Signal to Noise Ratio value for different sets of 10 images. Table 3 represents the Independent Sample T-Test is applied for the sample collections by fixing the level of significance as 0.005 with a confidence interval of 95%. After applying the SPSS calculation, Discrete Cosine Transformation has accepted a statistically significant value($p<0.05$). Figure 3, represents a simple graph where the X-axis is OpenCV vs Discrete Cosine Transformation and the Y-axis is the Mean of Peak Signal to Noise Ratio value detection which results in +/- 1SD

4. Discussion

The overall results show that there are some variations observed in the Peak Signal to Noise Ratio values which improved the image quality and embedding capacity. That proves the Discrete Cosine Transformation algorithm with a PSNR value of 52 is better than the OpenCV algorithm with a PSNR value of 46. There is a statistically significant difference in Image Steganography PSNR values of the two algorithms having a significant accuracy value of 0.001($p<0.005$ Independent sample T-Test) (Darbani, AlyanNezhadi, and Forghani 2019) an Image Steganography method for embedding text messages specifically in JPEG images. In this paper, the amount of capacity of secret data stored in the image is more. Also, the quality of the image is almost similar to the original image. Here, two adjacent pixels are considered where two less significant bits of each pixel are used for embedding. This is another approach that is used for Image Steganography. (Uruma et al. 2019) this paper proposed a method called novel approach to Image Steganography algorithm through image Colorization. The method embedded data into the null space of the colorization matrix. Using this matrix, a large capacity of data can be embedded into the image. The results of this paper proved that the capacity of image storage for data hiding is improved. (Jaradat, Taqieddin, and Mowafi 2021) the Image Steganography which has been developed in this paper is based on chaotic maps and the PSA algorithm. In this paper, the Peak Signal to Noise Ratio is improved drastically which is appreciable. Using this algorithm, the best pixel location is found and the data is embedded here for data hiding. The main motive of this paper was to improve the PSNR value, image quality, embedding capacity, and minimal distortion. (Nandi and Ghanti 2017) image Steganography is implemented with unique steps. The process is that firstly the text is encoded using the steps and then

embedded into the image. Similarly, the decoding process is done in the reverse process. So, the three steps are reversing, swapping, and circular right shifting for encoding whereas for decoding the steps are left circular shifting, swapping then reversing. The paper declares that using this method the data embedded in the image will not be lost. (Jangid and Sharma 2017; Rajput, Adhiya, and Patnaik 2017) audio Steganography is another type of Steganography that is being used to embed data for data hiding. In this paper, the algorithm used is the Least Significant Bit(LSB) algorithm. This paper aimed to increase storage capacity and security. The data embedded in the audio file is not embedded sequentially in a particular place, the data is embedded at specific points of the audio file. The proposed algorithm was better than the existing algorithm. (Velmurugan and Hemavathi 2019) similarly, in this paper, Audio Steganography is implemented but here it is implemented with a different algorithm. The algorithm used here is Neural Networks using a hash function to increase security. The main reason for using this algorithm is it is difficult to decode the steg-object. (Jangid and Sharma 2017) this paper implements Video Steganography by MLC(Multi-level clustering) algorithm. In this algorithm, K-means clustering is to cluster the cover frame. As a result, the Peak Signal to Noise Ratio is improved and the MSE value is reduced. The main motive of this paper was to improve PSNR value The Peak Signal to Noise Ratio is better than the OpenCV algorithm in the Discrete Cosine Transformation Algorithm(DCT) but the value is not efficient. There was an improvement but it is still not as required. Modifications in algorithms or using a different technique will improve Peak Signal to Noise Ratio value. And the message is easily lost if the image is subjected to compression. The comparison ratio must be improved to get better results. As Discrete Cosine Transformation is mostly compatible with JPEG image format, it must be made compatible for all different types of image formats. This tells us that the improvement in Steganography algorithms is important and necessary. Finally, if the above criteria are fulfilled then there will be an automatic improvement in image quality, embedding capacity, and Peak Signal to Noise Ratio value. Also, minimizing the distortion measure.

5. Conclusion

The paper aims to implement an innovative method for minimal distortion of Image Steganography. The Discrete Cosine Transformation(DCT) algorithm is better than the OpenCV algorithm because the Peak Signal to Noise Ratio value is higher in Discrete Cosine Transformation. The Peak Signal to Noise Ratio value is 52 and 46 in Discrete Cosine Transformation and OpenCV algorithms respectively. As the Peak Signal to Noise Ratio value increases, the image quality, and embedding capacity also increase. This will also lead to minimizing distortion. Therefore, the distortion is reduced to minimal using the innovative model.

Declarations

Conflict of Interests

No conflicts of interest in this manuscript.

Authors Contributions

Author ABL was involved in conceptualization, data collection, data analysis, manuscript writing. Author KM was involved in conceptualization, guidance, and critical review of the manuscript.

Acknowledgments

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

Funding: We thank the following organizations for providing financial support that enabled us to complete the study.

1. Metricbees Pvt.Ltd, Chennai.
2. Saveetha University
3. Saveetha Institute of Medical and Technical Sciences.
4. Saveetha School of Engineering.

6. References

Arun, Chandni, and Senthil Murugan. 2017. "Design of Image Steganography Using LSB XOR Substitution Method." In 2017 International Conference on Communication and Signal Processing (ICCSP). IEEE. https://doi.org/10.1109/iccsp.2017.8286444.

Darbani, Abbas, Mohammad M. AlyanNezhadi, and Majid Forghani. 2019. "A New Steganography Method for Embedding Message in JPEG Images." In 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI). IEEE. https://doi.org/10.1109/kbei.2019.8735054.

Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. 2020. "An Image Steganography Approach Based on K-Least Significant Bits (k-LSB)." In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE. https://doi.org/10.1109/iciot48696.2020.9089566.

Fridrich, Jessica. 2010. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press.

Jangid, Sachin, and Somesh Sharma. 2017. "High PSNR Based Video Steganography by MLC(multi-Level Clustering) Algorithm." In 2017 International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE. https://doi.org/10.1109/iccons.2017.8250530.

Jaradat, Aya, Eyad Taqieddin, and Moad Mowafi. 2021. "A High-Capacity Image Steganography Method Using Chaotic Particle Swarm Optimization." Security and Communication Networks 2021 (June). https://doi.org/10.1155/2021/6679284.

Kang, Hyun. 2021. "Sample Size Determination and Power Analysis Using the G*Power Software." Journal of Educational Evaluation for Health Professions 18 (July): 17.

Nandi, Biswarup, and Mousumi Ghanti. 2017. "Lossless Steganography: An Approach for Hiding Text under Image Cover." In 2017 International Conference on Inventive Computing and Informatics (ICICI). IEEE. https://doi.org/10.1109/icici.2017.8365389.

Pradhan, Anita, Aditya Kumar Sahu, Gandharba Swain, and K. Raja Sekhar. 2016. "Performance Evaluation Parameters of Image Steganography Techniques." In 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS). IEEE. https://doi.org/10.1109/rains.2016.7764399.

Rajput, Shital P., Krishnakant P. Adhiya, and Girish K. Patnaik. 2017. "An Efficient Audio Steganography Technique to Hide Text in Audio." In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). IEEE. https://doi.org/10.1109/iccubea.2017.8463948.

Sharma, Vipul, and Madhusudan. 2015. "Two New Approaches for Image Steganography Using Cryptography." In 2015 Third International Conference on Image Information Processing (ICIIP). IEEE. https://doi.org/10.1109/iciip.2015.7414766.

Sheidaee, Ali, and Leili Farzinvash. 2017. "A Novel Image Steganography Method Based on DCT and LSB." 2017 9th International Conference on Information and Knowledge Technology (IKT). https://doi.org/10.1109/ikt.2017.8258628.

Singh, Himanshu. 2019. "Advanced Image Processing Using OpenCV." Practical Machine Learning and Image Processing. https://doi.org/10.1007/978-1-4842-4149-3_4.

Swain, Gandharba. 2014. "Digital Image Steganography Using Nine-Pixel Differencing and Modified LSB Substitution." Indian Journal of Science and Technology. https://doi.org/10.17485/ijst/2014/v7i9.27.

Uruma, Kazunori, Katsumi Konishi, Tomohiro Takahashi, and Toshihiro Furukawa. 2019. "A Novel Approach to Image Steganography Based on the Image Colorization." 2019 IEEE Visual Communications and Image Processing (VCIP). https://doi.org/10.1109/vcip47243.2019.8965732.

Velmurugan, K. Jayasakthi, and S. Hemavathi. 2019. "Video Steganography by Neural Networks Using Hash Function." In 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM). IEEE. https://doi.org/10.1109/iconstem.2019.8918877.

Хорев, П. Б., and А. В. Сергеев. 2020. "Application of Steganography in the Corporate Environment." Информационно-технологический вестник, no. 4(26) (December): 104–9.

Tables and Figures

Table 1. Data collection from the N=10 sample of images to gain Peak Signal to Noise Ratio and reduce Mean Square Root for increase(%) of image quality and embedding capacity.

DataSet Sample (Different Images)	PSNR (OpenCV Algorithm)	PSNR (DCT Algorithm)
1	46.5	51.8
2	47.19	51
3	48.1	52.1
4	46	51.2
5	47	53
6	46	52.6
7	48	51.1
8	48.1	52.7
9	47.3	52
10	46.8	53.1

Table 2. This is group statistics for both algorithms. Comparison of the Peak Signal to Noise Ratio values of OpenCV and Discrete Cosine Transformation Algorithm. The highest PSNR value of OpenCV is (48.1) and the lowest is (46). The Discrete Cosine Transformation Algorithm has the highest PSNR value as (53.1) and the lowest is (51).

	Groups	N	Mean	Std.Deviation	Std.Error Mean
PSNR	**OpenCV**	10	47.0990	0.79848	0.25250
	DCT	10	52.0600	0.78344	0.24775

Table 3. Independent Samples T-Test is applied for the sample collections by fixing the level of significance as 0.05 with a confidence interval of 95%. After applying the SPSS calculation, the Discrete Cosine Transformation Algorithm has accepted a statistically significant value($p<0.05$).

		Levene's Test for Equality of Variances		T-Test for Equality of Means						
		F	Sig.	T	df	Sig. (2-tailed)	Mean Difference	Std.Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
PSNR	**Equal Variances assumed**	0	0.996	-14.024	18	0	-4.961	0.35374	-5.70419	-4.21781

	Equal Variances not assumed			-14.024	17.993	0	-4.961	0.35374	-5.70421	-4.21779

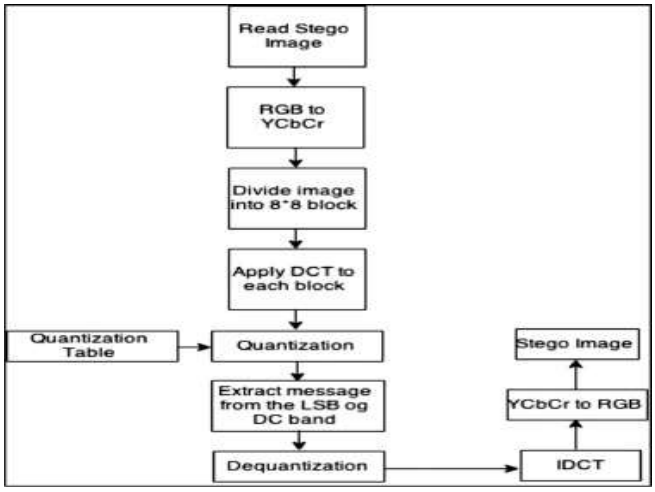

Fig. 1. Flowchart of Discrete Cosine Transformation Algorithm

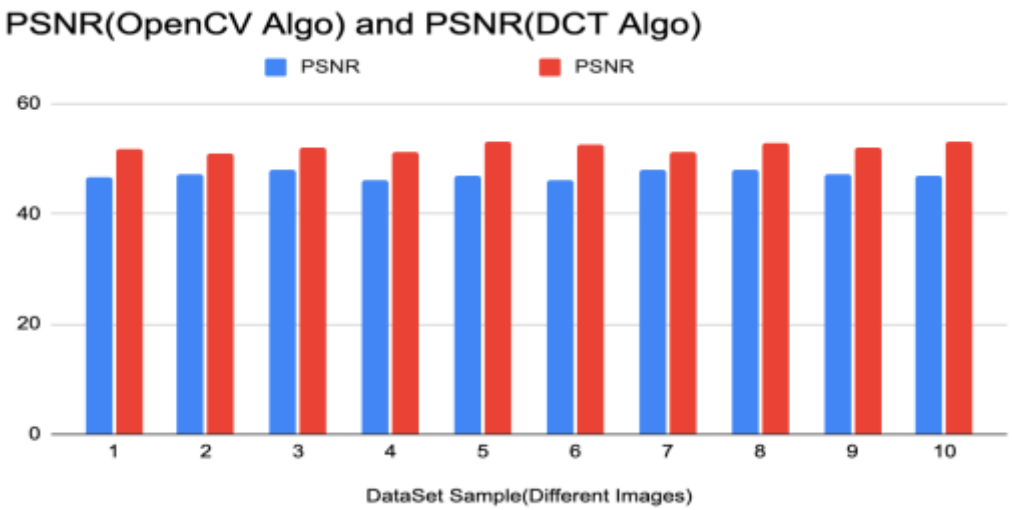

Fig. 2. A Comparison chart of Peak Signal to Noise Ratio values for Discrete Cosine Transformation algorithm and OpenCV algorithm.

Fig. 3. Bar graph between OpenCV and Discrete Cosine Transformation(DCT). Comparison of OpenCV and DCT in terms of PSNR values. The PSNR values of DCT are better than OpenCV.
X-Axis: OpenCV vs Discrete Cosine Transformation(DCT) Y-Axis: Mean of Peak Signal to Noise Ratio detection is +/- 1SD.