Comparative Analysis on the Image Steganographic Algorithms

Rosshini Selvamani, Yusliza Yusoff,
Nur Fatin Liyana Binti Mohd Rosely and Maheyzah Md Siraj

November 7, 2022

Comparative Analysis on the Image Steganographic Algorithms

Rosshini Selvamani
School of Computing
Universiti Teknologi Malaysia
Johor Bahru, Malaysia
srosshini98@gmail.com

Yusliza Binti Yusoff
School of Computing
Universiti Teknologi Malaysia
Johor Bahru, Malaysia
yusliza@utm.my

Nur Fatin Liyana Binti Mohd Rosely
Faculty of Data Science and Information Technology (FDSIT)
Inti Internation Universitiy
Nilai, Malaysia
fatinliyana.rosely@newinti.edu.my

Maheyzah Binti Sirat @ Md Siraj
School of Computing
Universiti Teknologi Malaysia
Johor Bahru, Malaysia
maheyzah@utm.my

Abstract*— As a result of recent technological advancements in digitalization, a vast amount of data is generated every day. With the increased usage of the Internet, it is becoming increasingly difficult to prevent black hat hackers from disclosing critical and secret information. As a result, this research contributes to identifying the best and most efficient algorithm from among the three opted image steganographic algorithms, which are Pixel Value Differencing (PVD), Optimum Pixel Value Adjustment Procedure (OPAP), and Discrete Cosine Transform (DCT), as well as the image format pairing that can facilitate the most data capacity while maintaining the highest image quality, resilience, and undetectability. The purpose of this research is to apply the three image steganographic algorithms to coloured and grayscale images in the PNG, JPG, and BMP formats. The research technique for the intended study activity is divided into three parts. Each step is intended to accomplish a certain goal. Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) were the two performance metrics utilized to evaluate the algorithms. For the experiment, seven (7) separate standard pictures of 512 x 512 pixels and 1024 x 1024 pixels in colour and grayscale are obtained and employed. The three algorithms were analysed, assessed, and compared at the end of this study in terms of robustness, capacity, and imperceptibility. In a nutshell, OPAP is the best and most efficient algorithm which can be used to conceal the secret text without affecting the image quality while OPAP works best with grayscale images of 1024 x 1024 px to produce an excellent output in terms of high robustness, imperceptibility, and capacity.

Keywords— Image steganographic algorithms, PVD, OPAP, DCT, robustness, capacity, imperceptibility.

I. Introduction

Every day, a massive amount of information is created as a result of recent technical developments in digitalization. With advancements in technology such as the Internet, knowledge is becoming more widely available. With the rising use of the Internet, it is difficult to avoid the disclosure of secret and sensitive information [1]. If the data provided is not securely transmitted to the intended recipients, it may result in a breach of privacy or dishonour that will take a long time to overcome. It is vital that any information shared or sent online be safe from hackers [3]. The best aspect is that there are numerous methods for maintaining data confidentiality. The need to safeguard the Internet against breaches in confidentiality, integrity, availability (CIA) is critical, and steganography plays an important role in creating a secure system.

Many services, such as the healthcare system, are afraid that unauthorised persons may get access to all of their secret and sensitive data. In terms of providing e-health services to patients, the healthcare system makes use of the Internet to simplify the interchange of digital medical pictures and data across health institutions. Medical records, diagnoses, scanned clinical examination photographs of patients, and other complicated datasets are all crucial components of any medical information system [2]. Because medical resources such as ultrasound scans, medical notes and X-ray pictures are critical in the treatment and diagnosis of a wide range of diseases, it is vital to ensure secure medical picture storage, processing, transmission and analysis of medical images while adhering to the healthcare data ethics policy. To meet the CIA standards, health officials are concentrating increasingly over the utilization of image steganography in digital medical images. Image steganography in medical photos attempts in order to embed large quantities of data in photographs in order to combine more vital patient data and to protect images. The amount of medical pictures exchanged through the Internet has increased dramatically in recent years, demanding extra capacity and data, as well as a secure communication method. The security of medical image is an important issue to address while keeping or sharing diagnostic information.

Nonetheless, by employing steganography, the sender goes a step further by insuring that no one would ever suspect the message existed. Steganography is the process of concealing information in ways that prohibit hidden signals from being discovered. Steganography is growing more important as more people become involved in present technological revolution. The goal of steganography is to keep secret data hidden from view [4]. Steganography may be divided into five (5) categories: image, text, video, audio, and network protocol. The file formats used are defined by the cover media that contains the concealed content. Digital photo, audio, and video are increasingly being marked with identifiable but invisible marks that may contain a hidden remark or unique identifier or even directly help in the prevention of illegal copying. Steganography is an effective security solution because of the different types of digital image formats that might be used, especially when combined with digital photographs [5].

Next, this paper contains the literature review of the three chosen image steganographic algorithms, research methodology incorporating experimental implementation design, data collection, performance measurements, and the evaluation parameters. Moreover, the results of the conducted experiment are presented along with the graphical presentations. Relevant comparisons and discussions are unveiled in this paper as well and concluded with the outcome of the experiment. The objective of this paper is to present the comparative experiment which then identifies the most efficient way of hiding secret texts within an image without diminishing the image quality.

II. Literature Review

This section has investigated and offered a comprehensive review of image steganography.

A. *Image Steganography*

Image steganography embeds a hidden message within image files of various formats, such as PNG, JPG, and BMP [6]. In steganography, images are the most commonly used file formats. They are known for producing a non-causal medium because of their capacity to access any pixel of the image at random. Additionally, the embedded data may be undetectable to the human eye [7]. Many studies and research on image steganography have been conducted in the past and continue to be conducted now. The following steganographic techniques for hiding data in pictures files are classified:

1. Spatial Domain
2. Frequency Domain
3. Adaptive.

1) Spatial Domain Steganography

This section shows the progression of well-known spatial steganography algorithms. It also integrates its quantitative and qualitative advantages and downsides. The spatial domain steganographic framework is immediately applied to the cover picture pixels [8]. Pixel Value Differencing (PVD) and Optimum Pixel Adjustment Procedure (OPAP) are two techniques in the spatial domain.

a) Pixel Value Differencing (PVD)

Wu and Tsai et al. [9] devised a steganographic approach based on pixel value difference to overcome the visual quality issue. The amount of bits to be injected is determined by the difference in value between two surrounding pixels. The method divides a cover picture into two non-overlapping consecutive pixel blocks in a zig-zag manner. Furthermore, in each block, the difference value between two pixels is evaluated to determine the concealing bit size, with difference values grouped into different ranges [10]. Human vision sensitivity is used to choose ranges or gaps in a range table. Finally, the concealed data is used to update the difference value with new difference value. The number of hidden messages depends on the structural area of a picture, which is controlled by table range levels. The larger the structural difference, the more hidden bits may be inserted in a pair of pixels. Generally, the PVD algorithms embeds more hidden data into pictures while maintaining visual undetectability [11].The peak signal-to-noise ratio (PSNR) value remains more than 40dB, allowing RS detection attacks to be avoided. 40dB of PSNR is considered good in terms of image quality. As of right now, there is no steganography method that can withstand every steganalysis attempt. The most significant steganalysis method is RS attack, that uses an algorithm to analyse pixel values statistically to find the steg-message

b) Optimum Pixel Value Adjustment (OPAP)

Chi-Kwon and L.M Cheng introduced this approach initially, and OPAP was created as an improvement on the least significant bit (LSB) - based technique [12]. OPAP is one of the well-defined approaches for picture data embedding. OPAP was designed to enhance the quality and security of stego-images generated by the LSB replacement technique [13]. The OPAP method adjusts the hidden bits in order to improve the overall visibility of the stego-image. The difference is determined by the pixel variations between the real stego-image pixels. This method is utilised for grayscale and coloured pictures, and it produces good overall imperceptibility. For common test pictures such as Baboon and Lena, the OPAP method was utilised to produce stego-images with high visual fidelity [10]. The pixel value is modified once the secret data has been hidden. This is done to increase the quality of the stego-image while preserving the message. This method has the advantage of producing a higher quality stego-image than the LSB replacement technique.

2) Frequency Domain Steganography

For the transform domain hiding system, a wide range of approaches have been proposed. When compared to time-domain hiding methods, strategies for concealing data in the frequency domain of a signal are significantly more enduring or persistent. Almost all reliable steganographic classifications currently work in the transform domain [14]. Frequency-based data transport systems use frequency transformations such as the Discrete Cosine Transform (DCT).

a) Discrete Cosine Transform (DCT)

DCT coefficients are calculated from an equation and quantized utilizing a specific Quantization Table (QT) in image and video processing. The message bits are supposed to be hidden by the picture DCT coefficients. This method produces an excellent stego-image [15]. DCT is used to mask data in critical areas of the cover picture. The importance of DCT is that it takes the corresponding input data and focuses its efforts on the first few transform components [16]. The picture is splitted into 8 by 8 pixel blocks, and the secret bits are hidden by altering the middle or high frequency. This method has the advantage of being more resistant to attacks like compression. To perform quantization in the transform domain, a typical quantization matrix is utilized. Following that, secret data is put in a zigzag manner at the changed domain’s LSB regions. The stego-image is then produced using 2D inverse DCT. Similarly, DCT and quantization are done sequentially in the stego-image at the receiver end, and data is recovered in a zigzag pattern from the LSB regions of the values [17]. Another advantage of this technique is that it produces a good PSNR, resulting in the highest-quality stego-image.

III. Experimental Implementation Design

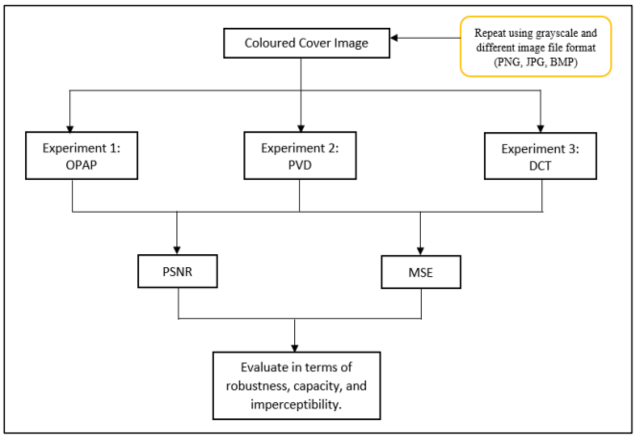
Coloured Cover Image
Repeat using grayscale and different image file format (PNG, JPG, BMP)
Experiment 1: OPAP
Experiment 2: PVD
Experiment 3: DCT
PSNR
MSE
Evaluate in terms of robustness, capacity, and imperceptibility.

Fig. 1. Framework of Overall Experiment Design

Figure 1 displays the overall framework structure of the research experiment. The very initial action is to upload a formatted coloured cover picture (PNG, BMP or JPG). The first method is then run to conceal the hidden message within the cover picture and generate the stego-image. After generating the stego-image, PSNR and MSE values are computed and assessed in terms of robustness, capacity, and imperceptibility. This entire flow is repeated using grayscale images and a different image format. The experiment will be conducted for 512 x 512 and 1024 x 1024 pixel images.

A. Data Collection

This experiment uses three distinct image formats as the cover images in this research. The cover media consists of seven (7) standard images. The images below are the cover images that were used as both coloured and grayscale images with pixel size of 512 x 512 and 1024 x 1024 throughout the experiment. Figure 2 below shows the coloured standard cover images while Figure 3 shows the grayscale images.

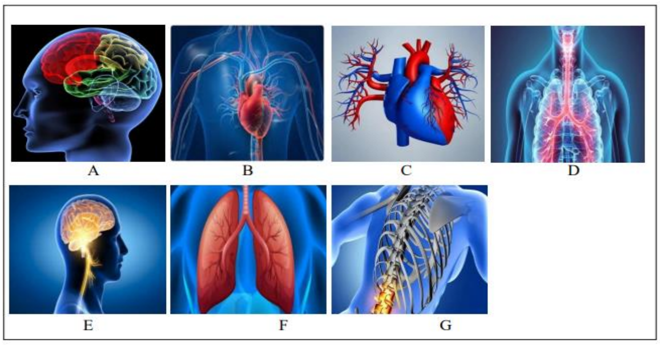

Fig. 2 Coloured Cover Images

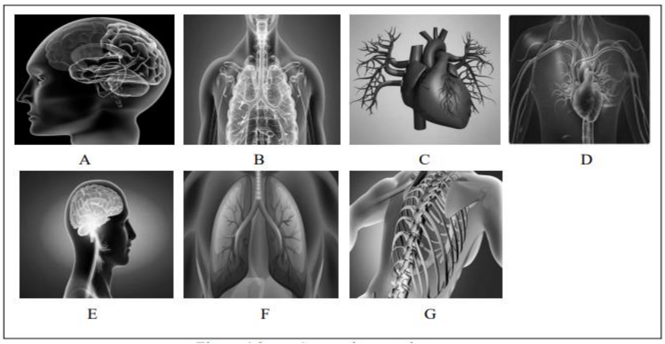

Fig. 3 Grayscale Cover Images

B. Peak Signal-to-Noise Ratio (PSNR)

PSNR is a widely used statistic for evaluating the degree of distortion in the cover picture induced by data hiding [5]. PSNR is defined as the ratio of a signal's maximum potential magnitude to its degree of noise caused by distortion (MSE). It is measured in decibels (dB). A solid PSNR must be more than 40 decibels. However, levels between 30 and 40 decibels are likewise acceptable. A higher PSNR value indicates better image quality [18]. The MSE value is required to determine the PSNR value. The PSNR calculation formula is shown below.

$$PSNR = 10 \text{ LOG}_{10} \frac{256 \times 256}{MSE} \tag{1}$$

C. Mean Square Error (MSE)

The MSE value is the mean amplitude of the square of the pixel-by-pixel variation between the real and stego-image [5]. It quantifies the error introduced into the cover picture as a result of the data hiding technique. The MSE should be as low as possible. This is because the lower the MSE number, the less the inaccuracy. The MSE value is 0 when the original and stego-image are identical. The MSE calculation formula is shown below.

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (pij - qij)2 \tag{2}$$

whereas, m, n = Image dimensions; *p* = Original image; q = Stego-image; i, j = Row and column numbers.

D. Robustness

Typically, robustness which is also known as resilience is evaluated in the transform domain, but different spatial domain techniques have recently been investigated when developing an algorithm. The term robustness refers to stego-capacity of image to preserve a hidden text although after it has been altered by different image processing procedures such as blurring, cropping, sharpening, and noise addition [19]. In other words, resilience is the capacity of an algorithm to retain the information disguised in the cover medium even after multiple changes have been applied to the cover [20]. It also refers to the amount of data that may be hidden without having any negative consequences or deleting the embedded data [21]. For the purpose of encrypting critical communications within images, high PNSR values lower the danger of the secret data being found that obliquely lowers the likelihood of an assault and thus providing high robustness.

E. *Embedding Capacity (EC)*

In comparison to the cover's size, the capacity is the quantity of message that may be concealed in it [19]. Another steganographic evaluation criterion is the number of secret bits encoded per pixel. These hiding bits per pixel (bpp) should preferably be as high as possible while maintaining visual quality and other evaluation metric concerns. The EC computation is shown below, where W and H are the image's width and height [19].

$$EC(bpp) = \frac{No.embedding\ bits}{W \times H} \qquad (3)$$

F. *Imperceptibility*

An outsider may discover the presence of concealed data in a specific file by computing and comparing several statistical features of the file to what is generally expected in that type of file [22]. As a result, imperceptibility is recognised as a significant performance measuring indicator in steganography. Steganographic techniques in general are sensitive to a variety of steganalysis detection attacks. Attackers are attracted to the stego-image in order to gain or even determine the existence of concealed data bits [19].

IV. Experimental Findings and Discussion

This section will present and discuss the results gained and gathered from the experiment, which was carried out utilizing three algorithms (PVD, OPAP, and DCT), three image formats (BMP, PNG, and JPG), 512 x 512 px and 1024 x 1024 px cover images in both coloured and grayscale forms. OPAP was implemented in Google Colaboratory while PVD and DCT were executed in Matlab. Tables and graphs are used to display the results.

1) *Comparative Result of 512x512 px with 1024x1024 px*

This section discusses the experimental result of the three algorithms (OPAP, PVD, and DCT) that was obtained from using seven different coloured and grayscale cover images of the size of 512 x 512 px and 1024 x 1024 px. 23 bytes sized secret text was hidden in each image where the PSNR and MSE values for each image were computed and compared.

a) Experimental Result Using Coloured Cover Images

This section displays the results of an experiment that was conducted using coloured cover images. Table 1 shows the Average PSNR and MSE values obtained from the experiment that was conducted for 512 x 512 px image A while Table 2 shows the values of 1024 x 1024 px image A.

TABLE I. PSNR AND MSE (COLOURED; 512 X 512 PX)

Average PSNR (dB) / MSE %				
Cover Image	**Image Format**	**OPAP**	**PVD**	**DCT**
A	.bmp	86.80 / 0	79.99 / 0	32.89 / 32.74
	.jpg	41.20 / 5.39	37.56 / 11.80	33.65 / 36.10
	.png	85.72 / 0	79.93 / 0	32.86 / 32.74

TABLE II. PSNR AND MSE (COLOURED; 1024 X1024 PX)

Average PSNR (dB) / MSE %				
Cover Image	**Image Format**	**OPAP**	**PVD**	**DCT**
A	.bmp	97.13 / 0	86.66 / 0	32.82 / 32.77
	.jpg	48.12 / 1.14	42.29 / 4.18	33.38 / 34.90
	.png	85.72 / 0	88.60 / 0	32.83 / 32.67

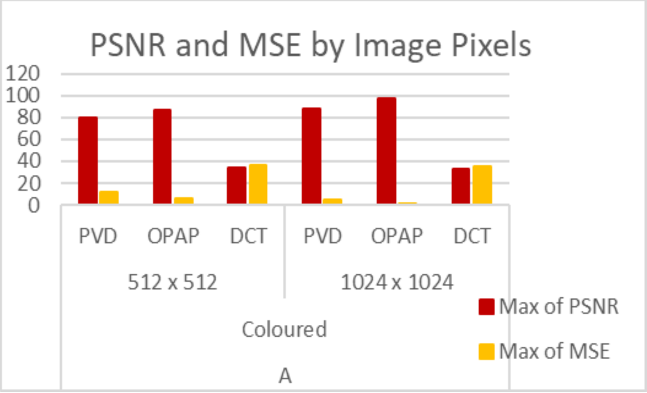

Fig. 4 PSNR and MSE Comparison (Coloured)

Figure 4 above presents the comparison between PSNR and MSE values of coloured images. Based on the Table 1, Table 2, and Figure 4, PSNR of 1024 x 1024 px images are higher for all algorithms namely, PVD, OPAP, and DCT as compared to the 512 x 512 px images. On the other hand, the MSE of 1024 x 1024 px images are lower than that of 512 x 512 px images. For 1024 x 1024-pixel images, OPAP records the highest PSNR and lowest MSE. This data shows the algorithms that used 1024 x 1024 px cover images produce higher quality stego-images with slightest differences from the original image. Hence, this concludes that 1024 x 1024 px coloured images are better to work along the algorithms as compared to coloured 512 x 512 px coloured images, OPAP specifically, to produce a better result in terms of higher robustness, imperceptibility, and embedding capacity.

b) Experimental Result Using Grayscale Cover Images

This section displays the results of an experiment that was conducted using grayscale cover images. Table 3 shows the Average PSNR and MSE values obtained from the experiment that was conducted for 512 x 512 px image A while Table 4 shows the values of 1024 x 1024 px image A.

TABLE III. PSNR AND MSE (GRAYSCALE; 512 X512 PX)

Average PSNR (dB) / MSE %				
Cover Image	**Image Format**	**OPAP**	**PVD**	**DCT**
A	.bmp	87.56 / 0	75.44 / 0	32.87 / 32.68
	.jpg	53.32 / 0.30	42.44 / 4.71	32.79 / 33.00
	.png	88.95 / 0	76.99 / 0	32.82 / 32.78

TABLE IV. PSNR AND MSE (GRAYSCALE; 512 X512 PX)

Average PSNR (dB) / MSE %				
Cover Image	**Image Format**	**OPAP**	**PVD**	**DCT**
A	.bmp	95.63 / 0	84.39 / 0	32.87 / 32.68
	.jpg	59.77 / 0.07	49.12 / 0.80	32.79 / 33.00
	.png	94.23 / 0	85.00 / 0	32.82 / 32.78

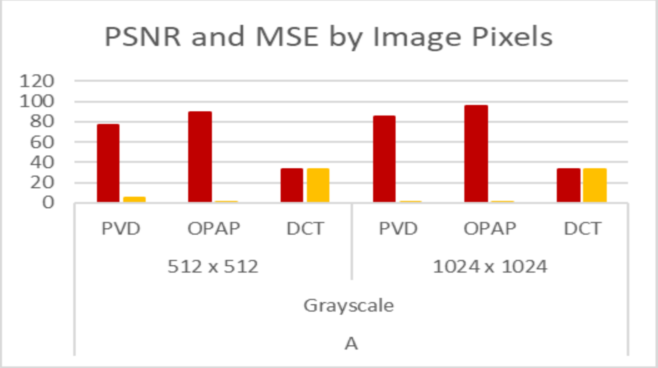

Fig. 5 PSNR and MSE Comparison (Grayscale)

Figure 5 shows a graphical presentation to show the comparison in results between grayscale images of 512 x 512 px and 1024 x 1024 px. Based on the figure above, PSNR of 1024 x 1024 px images are higher for all algorithms namely, PVD, OPAP, and DCT as compared to the 512 x 512 px images. On the other hand, the MSE of 1024 x 1024 px images are lower than that of 512 x 512 px images. For 1024 x 1024-pixel images, OPAP records the highest PSNR and lowest MSE. This data shows that the algorithms that used grayscale 1024 x 1024 px cover images produce higher quality stego-images with slightest differences from the original image. Hence, this concludes that 1024 x 1024 px grayscale images are better to work along the algorithms, OPAP specifically, to produce a better result in terms of higher robustness, imperceptibility, and embedding capacity.

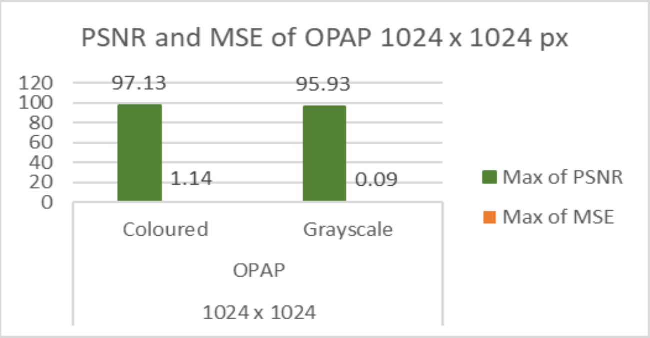

Fig. 6 PSNR Comparison (1024x1024 px)

Figure 6 exhibits a comparative result of OPAP using 1024 x 1024 px grayscale versus coloured images. Based on the comparison presented in Figure 6, coloured and grayscale 1024 x 1024 px images are chosen to contribute for better performances of algorithms. Next, Figure 5.15 shows that, between coloured and grayscale 1024 x 1024 px images in OPAP, grayscale 1024 x 1024 images in OPAP record lowest MSE and considerably high PSNR as compared to coloured 1024 x 1024 px images. Hence, grayscale 1024 x 1024 px images are the most compatible cover images to work with OPAP to produce a better result in terms of high robustness, imperceptibility, and embedding capacity.

c) Result Based on the 1024x1024 px Coloured Images with OPAP

This section presents the results of an experiment using 1024 x 1024 px coloured cover images. Figure 7 shows the average PSNR and MSE values generated from the experiment that was carried out using three algorithms, three image formats, and seven different coloured cover images.

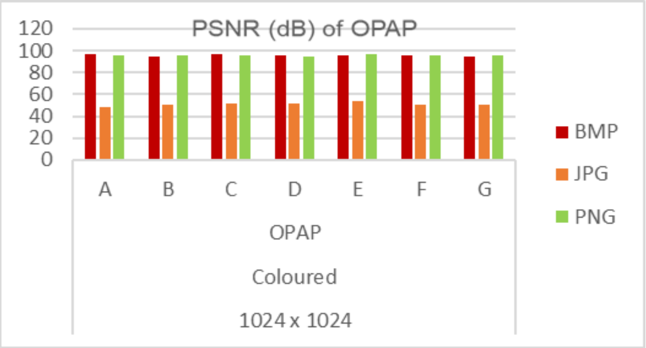

Fig. 7 PSNR of OPAP (Coloured; 1024x1024 px)

Figure 7 presents a graphical representation of OPAP PSNR values for all the seven (7) coloured cover images used. The aim is to determine the optimal image format to use along with OPAP in order to produce high-quality stego-images with increased resilience, imperceptibility, and embedding capacity. PNG images have the highest PSNR when compared to BMP and JPG. Four (4) out of seven (7) OPAP coloured BMP images have the greatest PSNR, followed by PNG and JPG. As a consequence, in terms of high resilience, imperceptibility, and embedding capacity for coloured 1024 x 1024 px images, OPAP and BMP are the best working algorithm and image format.

d) Result Based on the 1024x1024 px Grayscale Images with OPAP

This section presents the results of an experiment using 1024 x 1024 px grayscale cover images. Figure 7 shows the average PSNR and MSE values generated from the experiment that was carried out using three algorithms, three image formats, and seven different grayscale cover images

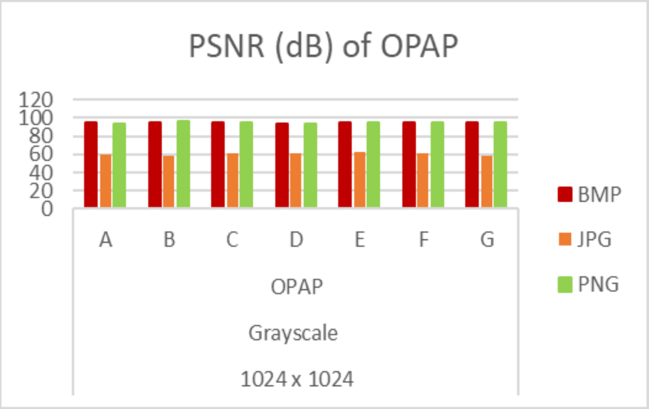

Fig. 8 PSNR of OPAP (Grayscale; 1024x1024 px)

Figure 8 presents a graphical representation of OPAP PSNR values for all the seven (7) grayscale cover images used. The aim is to determine the optimal image format to use along with OPAP in order to produce high-quality stego-images with increased resilience, imperceptibility, and embedding capacity. PNG images have the highest PSNR when compared to BMP and JPG. Six (6) out of seven (7) OPAP grayscale PNG images have the greatest PSNR, followed by BMP and JPG. As a consequence, in terms of high resilience, imperceptibility, and embedding capacity for grayscale 1024 x 1024 px images, OPAP and PNG are the best working algorithm and image format.

V. Conclusion

Based on the experiment that was conducted using coloured images, BMP is the most compatible image file format to be used along the OPAP algorithm. On the other hand, for the experiment that was carried out using grayscale images, OPAP and PNG are the best working algorithm and image file format. Finally, a comparison was made between the coloured and grayscale images of 512 x 512 px and 1024 x 1024 px images. Hence, it is concluded that grayscale 1024 x 1024 px images are the best working cover images with OPAP to produce a good outcome in terms of high robustness, imperceptibility, and embedding capacity. These parameters are compared and assessed based on the obtained PSNR and MSE values. According to the comparison analysis, OPAP is the best algorithm since it has the greatest PSNR value and the lowest MSE value when compared to PVD and DCT. OPAP is able of producing stego-images of the greatest quality in terms of robustness, capacity, and imperceptibility. Grayscale 1024 x 1024 px images record higher PSNR as compared to coloured 512 x 512 px images.

Acknowledgment

Special gratitude to the reviewers for their helpful guidance and suggestions. The authors are grateful to the Fundamental Research Grant (FRGS), Ministry of Higher Education Malaysia (MOHE) for financial support through grand Cost center Q.J130000.2551.20H71 UTM Fundamental Research Grant.. Thank you to the Research Management Center and School of Computing, Universiti Teknologi Malaysia (UTM) for thorough research support.

References

[1] A. K. Sahu And M. Sahu, “Digital Image Steganography And Steganalysis: A Journey Of The Past Three Decades,” Open Comput. Sci., Vol. 10, No. 1, Pp. 296–342, 2020, Doi: 10.1515/Comp-2020-0136.

[2] Dheyab, O. A. (2019). Hybrid Watermark Techniques For Skin Cancer Images (Doctoral Dissertation, Sultan Idris Education University).

[3] S. Venkatraman, A. Abraham, And M. Paprzycki, “Significance Of Steganography On Data Security,” Int. Conf. Inf. Technol. Coding Comput. Itcc, Vol. 2, No. May, Pp. 347–351, 2004, Doi: 10.1109/Itcc.2004.1286660.

[4] K. Vyas And B. L. Pal, “A Proposed Method In Image Steganography To Improve Image Quality With Lsb Technique,” Int. J. Adv. Res. Comput. Commun. Eng., Vol. 3, No. 1, Pp. 5246–5251, 2014.

[5] M. M. Hashim, M. S. M. Rahim, F. A. Johi, M. S. Taha, And H. S. Hamad, “Performance Evaluation Measurement Of Image Steganography Techniques With Analysis Of Lsb Based On Variation Image Formats,” Int. J. Eng. Technol., Vol. 7, No. 4, Pp. 3505–3514, 2018, Doi: 10.14419/Ijet.V7i4.17294.

[6] F. U. Mangla, S. Nokhaiz, M. Ramzan, And I. U. Lali, “International Journal Of Advanced And Applied Sciences A Novel Steganography Technique Using Grayscale Image Segmentation,” Vol. 6, No. 5, Pp. 84–91, 2019.

[7] A. Tiwary, “Different Image Steganography Techniques : An Overview International Journal Of Computer Engineering And Applications , Different Image Steganography Techniques : An Overview,” No. March, Pp. 0–13, 2019.

[8] R. Rq, Q. Dqg, J. Frp, And J. Frp, “, Pdjh 6sdwldo ’ Rpdlq 6whjdqrjudsk \ $ Vwxg \ Ri,” Vol. 6.

[9] D. C. Wu And W. H. Tsai, “A Steganographic Method For Images By Pixel-Value Differencing,” Pattern Recognit. Lett., Vol. 24, No. 9–10, Pp. 1613–1626, 2003, Doi: 10.1016/S0167-8655(02)00402-6.

[10] R. Amirtharajan, D. Adharsh., V. Vignesh., And R. J. B. Balaguru, “Pvd Blend With Pixel Indicator - Opap Composite For High Fidelity Steganography,” Int. J. Comput. Appl., Vol. 7, No. 9, Pp. 31–37, 2010, Doi: 10.5120/1275-1801.

[11] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, And K. H. Jung, “Image Steganography In

Spatial Domain: A Survey," Signal Process. Image Commun., Vol. 65, Pp. 46–66, 2018, Doi: 10.1016/J.Image.2018.03.012.

[12] R. Roy And S. Changder, "Quality Evaluation Of Image Steganography Techniques: A Heuristics Based Approach," Int. J. Secur. Its Appl., Vol. 10, No. 4, Pp. 179–196, 2016, Doi: 10.14257/Ijsia.2016.10.4.18.

[13] "Improved Hiding Data In Images By Optimal Moderately-Significant-Bit Replacement | Request Pdf." Https://Www.Researchgate.Net/Publication/3383826_Improved_Hiding_Data_In_Images_By_Optimal_Moderately-Significant-Bit_Replacement (Accessed Dec. 25, 2021).

[14] A. Yahya, Steganography Techniques For Digital Images. 2018.

[15] H. Singh, "Analysis Of Different Types Of Steganography," Int. J. Sci. Res. Sci. Eng. Technol., Vol. 2, No. 3, Pp. 578–582, 2016, [Online]. Available: Https://Pdfs.Semanticscholar.Org/62b4/8bd3c1f73aae78232e17e3dd0ebe7a7eaa90.Pdf.

[16] M. S. Subhedar And V. H. Mankar, "Current Status And Key Issues In Image Steganography: A Survey," Comput. Sci. Rev., Vol. 13–14, No. C, Pp. 95–113, 2014, Doi: 10.1016/J.Cosrev.2014.09.001.

[17] A. Chatterjee And N. Barik, "A New Data Hiding Scheme Using Laplace Transformation In Frequency Domain Steganography," Int. J. Hyperconnectivity Internet Things, Vol. 4, No. 1, Pp. 1–12, 2020, Doi: 10.4018/Ijhiot.2020010101.

[18] G. Maji And S. Mandal, "Secure And Robust Image Steganography Using A Reference Image As Key," Int. J. Innov. Technol. Explor. Eng., Vol. 8, No. 7, Pp. 2828–2837, 2019.

[19] A. A. Zakaria, M. Hussain, A. W. A. Wahab, M. Y. I. Idris, N. A. Abdullah, And K. H. Jung, "High-Capacity Image Steganography With Minimum Modified Bits Based On Data Mapping And Lsb Substitution," Appl. Sci., Vol. 10, No. 11, 2018, Doi: 10.3390/App8112199.

[20] S. Arunkumar, V. Subramaniyaswamy, And R. Logesh, "Hybrid Robust Image Steganography Approach For The Secure Transmission Of Biomedical Images In Cloud," Eai Endorsed Trans. Pervasive Heal. Technol., Vol. 5, No. 18, Pp. 1–12, 2019, Doi: 10.4108/Eai.13-7-2018.162401.

[21] R. Gupta, S. Gupta, And A. Singhal, "Importance And Techniques Of Information Hiding : A Review," Int. J. Comput. Trends Technol., Vol. 9, No. 5, Pp. 260–265, 2014, Doi: 10.14445/22312803/Ijctt-V9p149.

[22] S. Kingslin And N. Kavitha, "Evaluative Approach Towards Text Steganographic Techniques," Indian J. Sci. Technol., Vol. 8, No. 29, Pp. 1–8, 2015, Doi: 10.17485/Ijst/2015/V8i1/84415.