Article | Received 14 July 2023; Accepted 2 August 2023; Published 25 December 2023
https://doi.org/10.55092/pcs2023020046

# Comparative analysis of the spatial domain in digital image steganography

**Rosshini Selvamani *, Yusliza Yusoff, Razana Alwee, Suhaila Mohamad Yusuf, Zuriahati Mohd Yunos, Mohamad Shukor Talib, Haswadi Hasan**

Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia

* Correspondence author; Email: rosshini.s@graduate.utm.my.

**Abstract:** Digital steganography is a new and extremely demanding method for transmitting information securely over the internet while employing a covert device. Since its inception in the 1990s till the present, digital steganography has a lengthy history. Early steganography focused primarily on imperceptibility, security and embedding capacity. In addition to using statistics as a foundation, convolution neural networks (CNN), generative adversarial networks (GAN), coverless approaches, and machine learning are all used to construct steganographic methods. Robustness is becoming a crucial component of many innovative techniques. Spatial, Transform, and Adaptive domains serve as the understructure of those novel methods. This broadens the range of steganographic technique development and often concentrates the implementation of adaptive techniques. As a result, this study helps to analyze the fundamentals of image steganography, a comparative review on the spatial domain algorithms. As using evaluation tools is strongly tied to the effectiveness of steganography, this study also goes into great detail about its application. In order to demonstrate the effectiveness of spatial domain algorithms, the three competing spatial domain algorithms Least Significant Bit (LSB), Optimum Pixel Adjustment Procedure (OPAP), and Pixel Value Differencing (PVD) are being compared in this study to find the best and most efficient algorithm.

**Keywords:** image steganography; LSB; OPAP; PVD; spatial domain; comparative review

## 1. Introduction

Human existence is progressively moving into the digital sphere where the realm of the digital is becoming a larger part of human life. Public networks are becoming increasingly prevalent as a result of modern digitalization. Because of this, protecting the data via an unsecure public network is difficult. Unauthorized users, intruders, attackers, or enemies frequently have the ability to contaminate information by changing the message, leading to losses in money or reputation. Cybercrime is on the rise due to the need for digital data and

information exchanges. Therefore, security measures must also be established to guard against hacker assaults on transactions and information storage. Data protection techniques like encryption and data concealing are frequently employed. However, the two are distinct fields of study. Data concealment may be divided into three subcategories: cryptography, steganography, and watermarking. Steganography and cryptography both have the primary goal of preparing the hidden message for internet transport. Steganography runs counter to cryptography since it conceals sensitive information in media covers to deceive adversaries or hackers [1]. To preserve the proprietorship of the media cover, a watermark can be embedded using the watermarking technique. Nevertheless, the distinction between steganography and watermarking was inconsequential in the early stages of digital data concealment development. The degree of resilience and security of steganography were both negligible at the start of the creation of the watermarking technology [2,3].

As was already noted, the term "steganography" describes a method of communication concealment. It is a method that incorporates the covert message into the prominent host picture. In actuality, information concealment is a time-honoured concept that may even predate communication itself. Steganography literally translates to "cover writing" because its origins are in the Greek words "Stegos" and "grafia," which mean "cover" and "writing" [4]. With the development of updated communication technology, message transfer across various hosting mediums has become straightforward. With the advent of the internet, it became necessary to conceal sensitive information so that an intrusive party couldn't see it or recognize it [5]. By utilizing the image as a cover, it may be deduced that the concept of steganography initially relied on the least significant bit (LSB). However, other steganographic documents can also make use of a variety of covers, including audio, executable files (.EXE), and XML [6,7].

Steganography has been applied in the digital age in a variety of applications, including secure transfer, online banking, social networking, military, digital forensics, healthcare, online voting by QR code, telecommunication protocols, and biometric data [8–11]. In reality, steganography may be used for malicious purposes by those who aren't behind cyberattacks, or it might be used inadvertently. The Internet must be protected against compromises in its confidentiality, integrity, and availability (CIA), and steganography is crucial in building a secure system. Therefore, steganography science must be investigated in order to safeguard data and stop damaging cyber-attacks. Cyberattacks such as phishing are viewed as a severe security risk. Phishing is widespread in internet banking. Young, tech-savvy individuals have long been big fans of online banking, and as internet usage grows around the world and more people learn about its numerous advantages, that popularity is only going to increase. In any event, it may have disadvantages of its own. In a facility managing a bank account structure, there is a danger of running into a phoney label for exchange. An online account manager runs the risk of having a client's private key compromised and misused. Online transactions have increased over the past several years, which may be related to a number of assaults or security breaches. However, the sender goes a step further by using steganography to ensure that no one would ever be able to read the message.

The next portions of this study include a review of related literature on the three spatial domain algorithms that were chosen, research methodology, which includes experimental implementation design, data collection, performance measurements, and evaluation standards. Additionally, the experiment's outcomes are shown alongside the graphical representations. This study also makes pertinent comparisons and discussions, and it concludes with the experiment's findings. This study's goal is to offer a comparison experiment that determines the best technique for concealing sensitive text in images without compromising their quality.

There are five sections to the research. We quickly go over the foundations of image steganography in order to make the subject matter autonomous. We delve into further detail on literature of spatial domain and respective algorithms in Section 2. The performance measures and evaluation criteria are the primary focus of Section 3. In Sections 4 and 5, findings and conclusions are presented.

## 2. Literature review

The term “image steganography” refers to methods that can hide a steganographic message inside of an image such that it cannot be seen and deciphered by a third party. Image steganography refers to methods that can hide the steganographic message within an image such that a third party cannot decipher it. The picture files may be in many distinct formats, including PNG, JPG, and BMP [12]. Steganography attempts to hide the information, as opposed to cryptography, which modifies the data to render it unintelligible. The most common file types in steganography are images. They are recognized for creating a non-causal media because of their capacity to arbitrary access any pixel in the image. Imperceptibility or undetectability, embedding capacity, security, and robustness are the four primary criteria that are constantly assessed in data concealing. These four things serve as both the objectives and difficulties of data concealing research. Sometimes the elements are directly proportional to each other. The three different embedding domains of steganography are spatial, frequency or transformation, and adaptive.

### *2.1. Spatial domain*

The evolution of well-known spatial steganography methods is shown in this section. It also incorporates the benefits and drawbacks of both its quantitative and qualitative aspects. The secret message is inserted or embedded in this domain using the pixel's intensity. The embedding benefits of such a format are numerous. For instance, it boosts capacity with no restrictions and simplifies the system, which ensures the concealed message's imperceptibility [13]. In studies on image steganography, the spatial domain is most frequently employed. The ability to directly alter the pixel values of an image makes it reasonably easy to embed messages utilizing the spatial domain. If there is distortion or deformation in the stego-image, the spatial domain has the drawback that the message will be more brittle. Many researchers do assert that their approaches in the transform domain have a great capacity, however when these methods are examined, it is shown that they

employ non-blind extraction. Several of the extensively used and developed spatial approaches include LSB, OPAP, and PVD.

*2.2. Least significant bit (LSB)*

The simplest method is the Least Significant Bit (LSB) approach, which modifies the least significant bit of a specific quantity of pixels in the image to encode the message [14]. One of the first LSB-based approaches was the LSB replacement (LSB-r) method, which replaced a section of the picture's pixels' less-important bits with a steganographic message. Other methods include LSB matching (LSB-m), which modifies a number of pixels by adjusting the LSB value to match the bits in both the steganographic message and the image. Research [15] served as the method's original inspiration, and it was later refined in the 1990s and is constantly being improved upon today. Moreover, when embedding messages, the LSB technique may be used in conjunction with transformation domain techniques. Due to its improved imperceptibility and capacity, as well as its greater resistance to specialized steganalysis assaults, the evolution of the LSB technique is unquestionably far more secure than the original LSB approach. Figure 1 below depicts the mechanism of LSB.

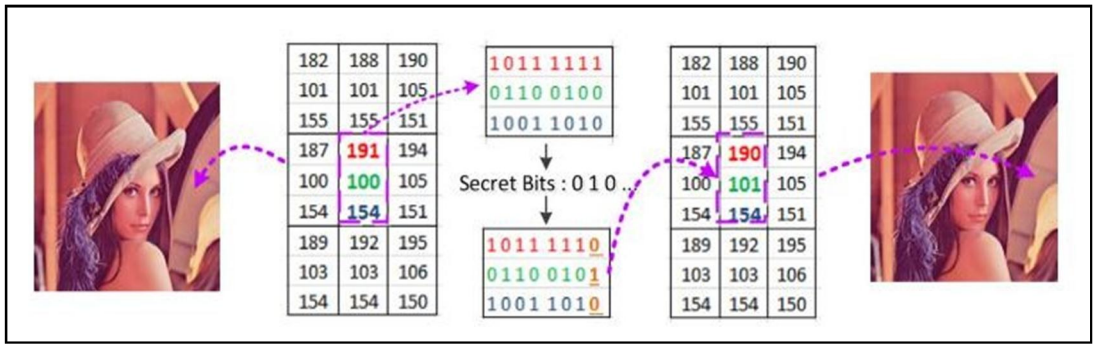


**Figure 1.** LSB mechanism.

*2.3. Optimum pixel adjustment procedure (OPAP)*

This method was first established by Chi-Kwon and L.M. Cheng, where OPAP was developed as an advancement over the LSB-based methodology [15,16]. One of the established methods for embedding image data is OPAP. The major goal was to enhance the stego- image's quality while reducing the computational complexity involved in changing four LSB bits to conceal the secret data [17,18]. The pixel differences between the actual stego-image pixels are what make the difference. This technique generates good overall imperceptibility and is used for both coloured and grayscale images. The secret info is concealed before changing the pixel value. By doing this, the message is maintained while the stego-image quality is improved. The benefit of using this method over the LSB replacement technique is that it creates stego-images of greater quality.

### *2.4. Pixel value differencing (PVD)*

Wu and Tsai were the ones who first created the PVD process [19]. The concept is to quantize the difference in neighbouring pixel values and then insert a hidden message based on the results. The technique creates two non-overlapping successive pixel blocks out of a cover image in a zig-zag pattern. Additionally, each block's concealing bit size is determined by evaluating the difference value between two pixels, which is divided into several ranges [20]. The selection of ranges or gaps in a range table is based on the human visual sensitivity. Two pixels' worth of information in the horizontal direction is used by default to estimate the difference. Due to its greater capacity and resistance to RS analysis attacks, this approach is more secure than LSB. In order to prevent RS detection assaults, the peak signal-to-noise ratio (PSNR) value must be higher than 40dB. In terms of visual quality, 40dB of PSNR is regarded as good. There is currently no steganography technique that can survive all steganalysis attempts. The PVD-based approach often has superior imperceptibility than LSB based on Human Visual System (HVS) measurement instruments like SSIM. However, pixel difference histogram (PDH) assaults are poor against the PVD standard. PVD was created using a variety of techniques, including the modulus function (MF), to enhance security, imperceptibility, and payload [21].

## 3. Experimental implementation design

The general framework structure of the study investigation is illustrated in Figure 2. Uploading a prepared, coloured cover image (PNG, BMP, or JPG) is the first step. The first approach is then used to produce the stego-image and hide the generated concealed text within the cover image. The stego-image is created, and the PSNR and MSE values are calculated and evaluated for robustness, capacity, and imperceptibility. Using grayscale photographs and a new image format, the entire procedure is repeated. The experiment will be conducted on images that are 1024 x 1024 pixels in size.

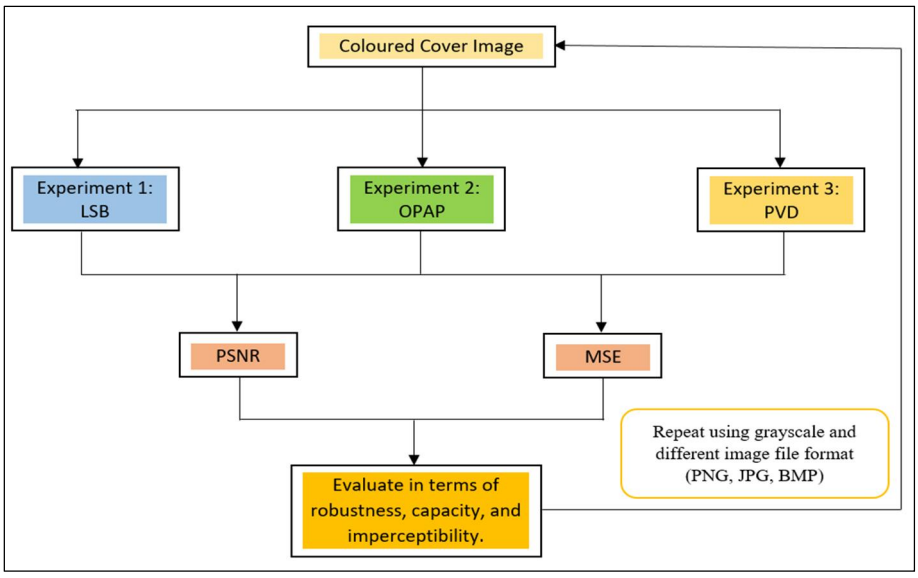


**Figure 2.** General framework of study.

*3.1. Data collection*

Three different picture formats are used as the research's cover images in this experiment. The cover material is made up of four (4) standard pictures. Throughout the test period, the cover pictures Lena, Tiffany, Baboon, and Peppers with pixel sizes of 1024 x 1024 as shown below in Figure 3 were used in the intended research as the cover images in both grayscale and colour. The USC SIPI Volume 3: Miscellaneous website (https://sipi.usc.edu/database/database.php?volume=misc) is where this dataset was retrieved from. The steganographic technique with target imperceptibility and payload capability is where this dataset is most frequently employed.

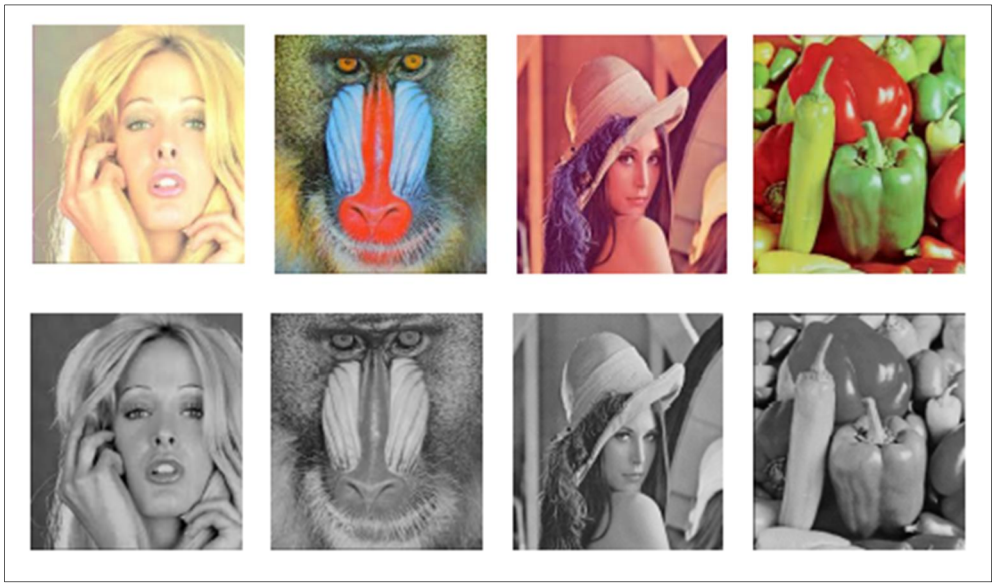

**Figure 3.** Standard cover images.

*3.2. Performance measures*

The primary domain and steganography techniques are summarized in the preceding section. There are several algorithms with various benefits and drawbacks within this and other domains. This experiment focuses on imperceptibility, embedding capacity, robustness, and security. Though, various techniques have been suggested in the literature to assess the effectiveness of steganographic approaches. The categorization proposed by past researchers may be broken down into the following groups [16,22–24].

3.2.1 Visual quality

If the steganographic message is inserted, many measures may be used to determine whether the image quality has not been affected. Calculating the Euclidean Distance between each pixel of both pictures is the easiest method. The Image Quality Index, Structural Similarity Image Quality Assessment, Image Fidelity, or the Mean Difference are other metrics examined in the most recent research.

3.2.2 Embedding capacity

The size of the hidden message that may be included into the cover picture is referred to as the payload capacity. The efficiency of the steganography method increases with the payload capacity since fewer covers are needed to convey messages. However, the influence on the imperceptibility factor tends to increase with payload size [24].

3.2.3 Security

Evaluates the capacity to evade a detection assault, which entails obtaining information from the picture to determine if it conceals information.

3.2.4 Imperceptibility

Once the message has been integrated, imperceptibility is utilized to gauge the impact of distortion on the cover picture. The quality of a picture can be affected by excessive distortion, which may even be visible to the human eye.

3.2.5 Robustness

The phrase "robustness" describes an image's ability to retain a hidden text even after it has undergone several image-processing techniques as blurring, cropping, sharpening, and noise addition [22]. Resilience, in other words, is the algorithm's ability to hold onto the information masked in the cover medium even after several modifications have been made to the cover [23]. Additionally, it relates to the volume of data that may be concealed without causing any harm or erasing the contained data [24]. High PNSR values reduce the risk of the secret data being discovered, which is necessary for the encryption of crucial messages inside pictures.

3.2.6 Computational complexity

Measures the number of operations required to conceal and retrieve the steganographic message as well as the execution time. It is better to select techniques that take less time to execute.

*3.3. Evaluation criteria*

A range of measures will be used to evaluate the performance of the created stego-image steganography system.

3.3.1 Peak signal-to-noise ratio (PSNR)

The PSNR metric is frequently used to assess the level of cover image distortion brought on by data concealing [12]. The greatest possible magnitude of a signal to the amount of noise it generates due to distortion (MSE) is known as PSNR. Decibels (dB) are used to express it. More than 40 dB is required for a strong PSNR. The permissible range is between 30 and 40

dB, though. Better image quality is indicated by a higher PSNR value [25]. The PSNR value can only be calculated with the MSE value. The algorithm for calculating PSNR is shown below.

$$PSNR = 10\ (\frac{255\ \times 255}{MSE}) \tag{1}$$

3.3.2 Mean square error (MSE)

The mean square of the pixel-by-pixel difference between the actual and stego-image is the MSE value [25]. It measures the inaccuracy that the data concealing strategy caused to appear on the cover image. MSE ought to be as little as feasible. This is due to the fact that accuracy is inversely correlated with MSE number. When the original and stego-image are identical, the MSE value is 0. The formula for calculating MSE is shown below.

$$\frac{1}{mn}\sum_{i=0}^{m-1}\ \sum_{j=0}^{n-1}\ [I(i,j) - K(i,j)] \tag{3}$$

## 4. Findings and discussion

The research experiment was conducted using three algorithms (LSB, OPAP, and LSB) of three picture file types (BMP, PNG, and JPG), of size 1024 x 1024 cover images in both coloured and grayscale forms. The results will be presented and discussed in this section. While LSB and PVD were run through Matlab, OPAP was carried out in Google Colaboratory. The outcomes are displayed using graphical images.

### *4.1. Outcome of PSNR and MSE for coloured images*

The experimental results of the three algorithms, LSB, OPAP, and PVD of pixel size 1024 by 1024 coloured images are discussed in this subsection. Figure 4 and Figure 5 below show the average result of PSNR and MSE based on the algorithms and picture file formats BMP, PNG, JPG accordingly. Based on the Fig. 4, OPAP algorithm records the highest level of PSNR followed by LSB, PVD algorithms while for the picture format, PNG has the highest PSNR value as compared to BMP, JPG. Contrarily, based on Fig. 5, MSE of OPAP algorithm records the lowest as it should be compared to LSB and PVD. On the other hand, JPG has the lowest MSE values but values of PNG and BMP are not further different. Considering both the PSNR and MSE values, it can be said that OPAP has the highest PSNR and lowest MSE which indirectly means OPAP is the most efficient algorithm than LSB and PVD.

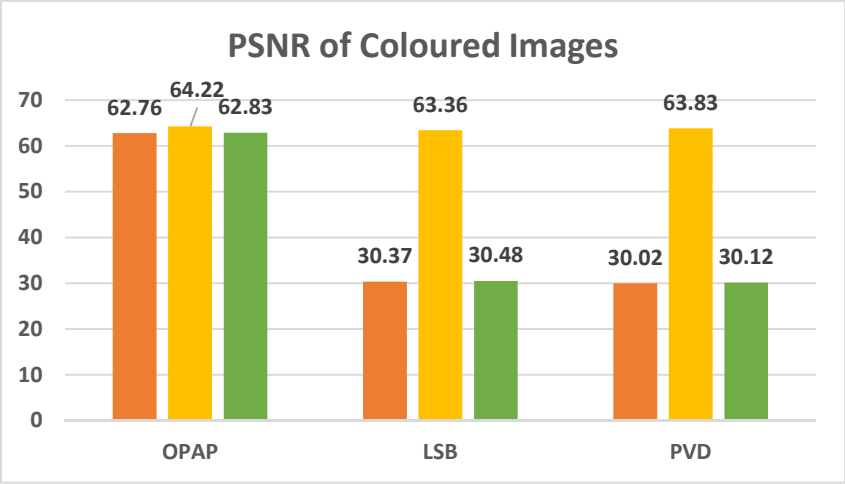


**Figure 4.** PSNR of coloured images based on image formats.

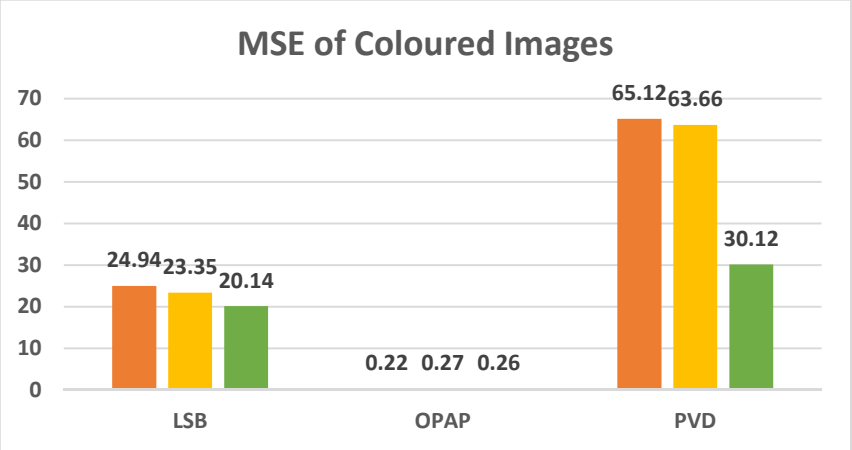


**Figure 5.** MSE of coloured images based on image formats.

*4.2. Comparative result for coloured versus grayscale images*

This section displays and discusses the comparative result of PSNR and MSE for coloured images with the ones of grayscale images. Based on Figure 6 below, both coloured and grayscale images have relatively high PSNR values, therefore it comes down to the MSE values which indicates the difference of stego-image from the original standard image. In that case, grayscale images are better than coloured images due to the great picture quality and lower MSE value as compared to coloured images.

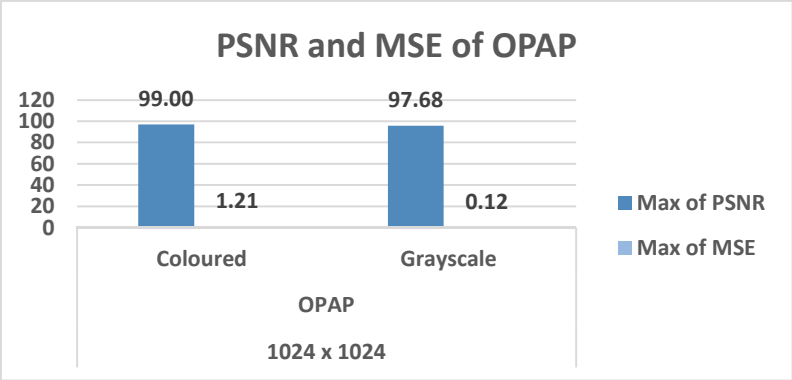


**Figure 6.** Comparison of PSNR and MSE of OPAP.

*4.3. Comparative result for coloured versus grayscale images*

This part of the section compares the result of OPAP algorithm using grayscale images given it has been proven that grayscale images are better than coloured in terms of the difference between original and stego-images. This result is presented based on the image file formats BMP, JPG, and PNG to identify the most suitable and compatible image type to be employed. Figure 7 below clearly shows JPG creates the lowest quality stego-image which makes leaves BMP and PNG. Out of 4 images. 3 PNG images record comparatively higher PSNR values than BMP. Eventhough BMP has competitive values as PNG, in terms of producing the greatest quality of stego-image, PNG is the most suitable. Figure 8 below displays the output PNG stego-images using OPAP algorithm in both coloured and grayscale. From the picture, the output images look relatively similar to the original images with less distortion and great image quality.

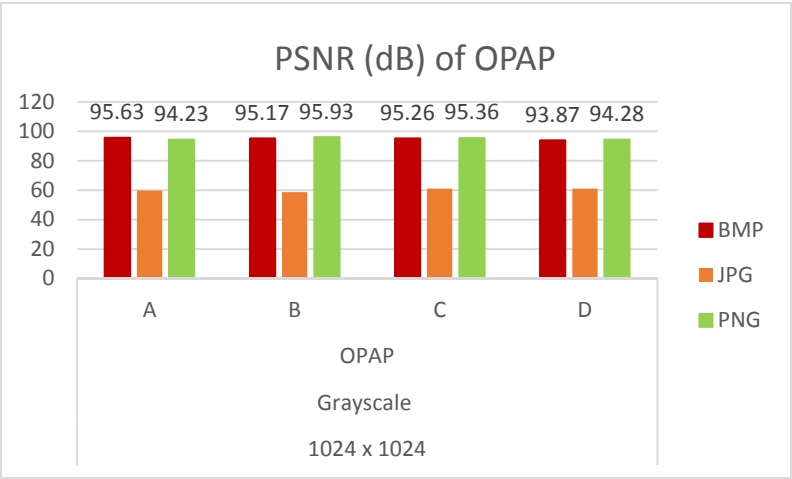


**Figure 7.** PSNR of grayscale images based on image formats.

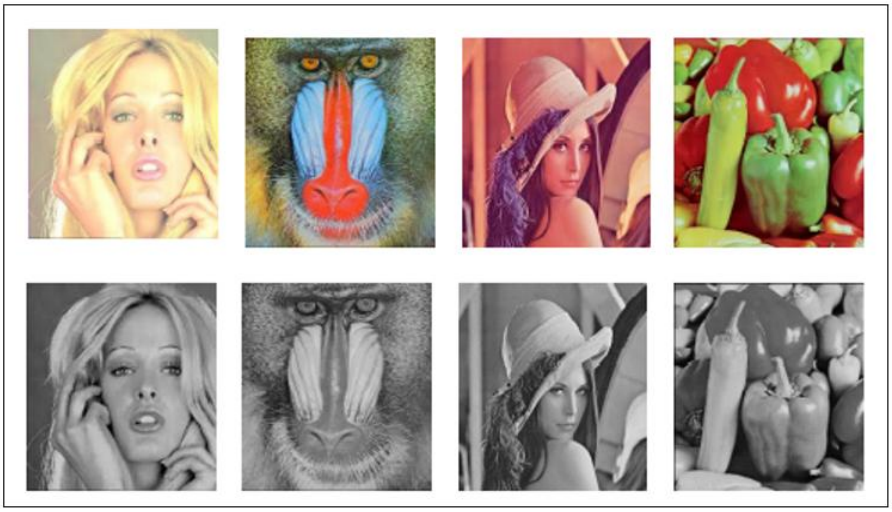

**Figure 8.** Standard cover images.

## 5. Conclusion

In a nutshell, spatial domain has a major potential as the base or starting point of an enhanced and successful image steganographic algorithm due to its simple yet efficacious manner. It is able to produce a high quality stego-image with high embedding capacity and imperceptibility through achieving a high PSNR and low MSE. From the comparative experiment that was conducted, it is concluded that OPAP is the best algorithm as compared to LSB and PVD due to its ability to provide high quality secured stego-image with 64.22 PSNR and 0. 27 MSE values. The work of steganography system enhancement is ongoing. This effort brought up a few additional directions worth exploring in the future. For instance, combining the spatial domain with frequency domain and methods such as machine learning and deep learning might increase security. By doing this, the security and robustness may be improved. The most significant flaw in the steganography technology has to do with the expansion of the secret message's carrying capacity. It is challenging to develop the steganography due to the limitations of the secret message using PSNR. In this case, handling the secret message beforehand and making it dynamic with the embedding technique is preferable. This makes the pre-processing stage collaborative with the concealment process.

## Acknowledgements

Special appreciation to reviewers for useful guidance and comments. The authors would like to acknowledge Ministry of Higher Education Malaysia (MOHE) under Fundamental Research Grant Scheme (FRGS) (Ref: FRGS/1/2021/ICT07/UTM/02/5) vote R.J130000.7851.5F462 and Research Management Center (RMC) of Universiti Teknologi Malaysia (UTM).

## References


[1] Gambhir A, Khushboo, Arya R. *Performance analysis and implementation of DES algorithm and RSA algorithm with image and audio steganography techniques*; Iyer B, Nalbalwar SL, Pathak NP, Eds. Advances in Intelligent Systems and Computing. Singapore: Springer, 2019, pp. 1021-1028.

[2] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. *Signal Process*. 2010, 90(3):727-752.

[3] Majeed MA, Sulaiman R, Shukur Z, Hasan MK. A review on text steganography techniques. *Mathematics*. 2021, 9(21):2829.

[4] Laxmi KR, Ramya N, Pallavi S, Madhuravani K. *Study and Analysis of Apriori and K-Means Algorithms for Web Mining*; Saini HS, Singh RK, Beg MT, Sahambi JS, Eds. Lecture Notes in Networks and Systems. Singapore: Springer, 2020, pp. 693-701.

[5] Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*. 2019, 335:299-326.

[6] Hosmer C. Discovering hidden evidence. *J Digit Forensic Pract*. 2006, 1(1):47-56.

[7] Hernandez-Castro JC, Blasco-Lopez I, Estevez-Tapiador JM, Ribagorda-Garnacho A. Steganography in games: A general methodology and its application to the game of Go. *Comput Secur*. 2006, 25(1):64-71.

[8] Mohsin AH, Zaidan AA, Zaidan BB, Ariffin SA, Albahri OS, *et al.* Real-time medical systems based on human biometric steganography: A systematic review. *J Med Syst*. 2018, 42:1-20.

[9] Douglas M, Bailey K, Leeney M, Curran K. An overview of steganography techniques applied to the protection of biometric data. *Multimed Tools Appl*. 2018, 77(13):17333-73.

[10] Chakkaravarthy SS, Sangeetha D, Vaidehi V. A survey on malware analysis and mitigation techniques. *Comput Sci Rev*. 2019, 32:1-23.

[11] Aos AZ, Naji AW, Hameed SA, Othman F, Zaidan BB. Approved undetectable-antivirus steganography for multimedia information in PE-file. In *2009 International Association of Computer Science and Information Technology-Spring Conference*, Singapore, April 17-20, 2009, pp. 437-441.

[12] Hashim MM, Rahim MS, Johi FA, Taha MS, Hamad HS. Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *Int J Eng Technol*. 2018, 7(4):3505-3514.

[13] Gutub A, Al-Ghamdi M. Image based steganography to facilitate improving counting-based secret sharing. *3D Res*. 2019, 10:1-36.

[14] Neeta D, Snehal K, Jacobs D. Implementation of LSB steganography and its evaluation for various bits. In *2006 1st International Conference on Digital Information Management*, Bangalore, India, December 6-8, 2006, pp. 173-178.

[15] Kurak Jr CW, McHugh J. A cautionary note on image downgrading. In *[1992] Proceedings Eighth Annual Computer Security Application Conference*, San Antonio, USA, November 30-December 4, 1992, pp. 153-159.

[16] Hussain M, Wahab AW, Idris YI, Ho AT, Jung KH. Image steganography in spatial domain: A survey. *Signal Process Image Commun*. 2018, 65:46-66.

[17] Turitsyna EG, Webb S. Simple design of FBG-based VSB filters for ultra-dense WDM transmission. *Electron Lett*. 2005, 41(2):1.

[18] Darabkh KA, Al-Dhamari AK, Jafar IF. A new steganographic algorithm based on multi directional PVD and modified LSB. *Inf Technol Control*. 2017, 46(1):16-36.

[19] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. *Pattern Recognit Lett*. 2003, 24(9-10):1613-1626.

[20] Amirtharajan R, Adharsh D, Vignesh V, Balaguru RJ. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. *Int J Comput Appl*. 2010, 7(9):31-37.

[21] Pradhan A, Sekhar KR, Swain G. Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks. *Secur Commun Netw*. 2017, 2017.

[22] Zakaria AA, Hussain M, Wahab AW, Idris MY, Abdullah NA, Jung KH. High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. *Appl Sci*. 2018, 8(11):2199.

[23] Arunkumar S, Subramaniyaswamy V, Logesh R. Hybrid Robust Image Steganography approach for the secure transmission of biomedical images in Cloud. *EAI Endorsed Trans Pervasive Health Technol*. 2019, 5(18):e1.

[24] Gupta R, Gupta S, Singhal A. Importance and techniques of information hiding: A review. *arXiv* 2014, arXiv:1404.3063.

[25] Maji G, Mandal S. Secure and robust image steganography using a reference image as key. *Int J Innov Technol Explor Eng (IJITEE)*. 2019, 8(7):2828-2839.