QUBAHAN ACADEMIC JOURNAL
VOL. 4, NO. 1, March 2024
https://doi.org/10.48161/qaj.v4n1a421

Effectiveness of the Spatial Domain Techniques in Digital Image Steganography

Rosshini Selvamani [1] and Yusliza Yusoff [2]

[1, 2] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia;

Corresponding author: e-mail: 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. The purpose of this research is to determine the best and most effective algorithm among the three competitive spatial domain algorithms, which are Least Significant Bit (LSB), Optimum Pixel Adjustment Procedure (OPAP), and Pixel Value Differencing (PVD) which in regard demonstrated the efficacy of spatial domain algorithms.

Keywords: Spatial domain, Least Significant Bit (LSB), Optimum Pixel Adjustment Procedure (OPAP), Pixel Value Differencing (PVD), Efficacy.

I. INTRODUCTION

Human life is increasingly intertwined with the digital realm, where digitalization plays an expanding role. With the prevalence of public networks, securing data over unsecure public networks becomes a challenge. Unauthorized individuals can tamper with information, leading to financial or reputational losses. The rise of cybercrime underscores the importance of security measures for safeguarding transactions and data storage. Encryption and data concealment techniques are frequently employed, although they are distinct fields. Data concealment encompasses cryptography, steganography, and watermarking as subcategories. While steganography and cryptography both prepare hidden messages for online transmission, steganography differs by concealing sensitive data within media covers to deceive adversaries [1]. Watermarking can embed a watermark in media covers to assert ownership. However, the distinction between steganography and watermarking was initially unclear, and their resilience and security were limited in the early stages of digital data concealment development [2,3].

Steganography, meaning "cover writing" from the Greek terms "Stegos" and "grafia" (cover and writing), involves embedding covert messages within prominent host images. This practice, dating back to ancient times, gained renewed importance with the internet's emergence [4]. Modern communication technology necessitated the concealment of sensitive information from prying eyes [5]. Initially, steganography relied on techniques like the least significant bit (LSB) to utilize images as covers, but it has since expanded to encompass various other media, including audio, executable files (.EXE), and XML [6,7].

Steganography has found applications in secure transfers, online banking, social networking, military operations, digital forensics, healthcare, online voting via QR codes, telecommunication protocols, and biometric data [8, 9, 10, 11]. Unfortunately, steganography can also be misused for malicious purposes or inadvertently employed. Safeguarding the confidentiality, integrity, and availability (CIA) of the internet is crucial, and steganography plays a vital role in building a secure system. As a result, research into steganography is necessary to protect data and prevent damaging cyberattacks. Phishing attacks, for instance, pose a significant security threat, particularly in internet banking, where users' private keys can be compromised. Steganography provides an extra layer of security by ensuring that messages remain undecipherable [12].

The following parts of this research consist of an examination of three chosen spatial domain algorithms, the study's approach, which encompasses experimental planning, data gathering, performance assessments, and assessment standards. The study presents experimental results and graphical representations, followed by relevant comparisons and discussions, concluding with the study's findings. The aim of this research is to conduct a comparative experiment to determine the most effective technique for concealing sensitive text within images without compromising their quality.

II. LITERATURE REVIEW

The term "image steganography" pertains to techniques for concealing a steganographic message within an image in such a way that it remains invisible and indecipherable to third parties. Image steganography involves concealing the steganographic message within an image to prevent third-party decryption. These images can exist in various formats, including PNG, JPG, and BMP [12]. Unlike cryptography, which alters data to make it unintelligible, steganography aims to hide information. Images are the preferred file types for steganography due to their non-causal nature and the ability to access any pixel in the image randomly. Data concealment is continually assessed based on four primary criteria: imperceptibility or undetectability, embedding capacity, security, and robustness. These criteria simultaneously serve as both the objectives and challenges of data concealment research and are sometimes interrelated. Steganography employs three distinct embedding domains: spatial, frequency or transformation, and adaptive.

In spatial domain, the secret data is embedded using the pixel's intensity, offering several advantages. For example, it enhances capacity without limitations and simplifies the system, ensuring the message remains imperceptible [13]. Spatial domain techniques are widely employed in image steganography research due to their ability to directly modify pixel values, making message embedding relatively straightforward. However, a drawback of the spatial domain is that the message becomes more fragile in the presence of stego image distortion or deformation. While some researchers claim that their transform domain approaches offer high capacity, upon examination, it becomes evident that they rely on non-blind extraction methods. Notable spatial techniques that have been extensively used and developed include LSB, OPAP, and PVD.

The simplest application to steganography is the Least Significant Bit (LSB) method, which involves adjusting the least significant bit of a specific number of pixels in an image to conceal a message [14]. One of the earliest LSB-based techniques is the LSB replacement (LSB-r) method, which replaces the steganographic message with the least significant bit of a subset of the pixels in the image. Another technique known as LSB matching (LSB-m) modifies multiple pixels by adjusting the LSB to match the bits in both the steganographic message and the image. This method was initially inspired by research [15] and has undergone refinements since the 1990s, continuously improving to this day.

Furthermore, the LSB technique can be used in conjunction with transformation domain techniques when embedding messages. Thanks to its enhanced imperceptibility, capacity, and greater resistance to specialized steganalysis attacks, the evolution of the LSB technique is undoubtedly more secure than the original LSB approach.

OPAP approach was initially pioneered by Chi-Kwon and L.M. Cheng, leading to the development of OPAP as a significant advancement beyond the LSB-based approach [15]. OPAP stands out as one of the established methods for embedding image data. Its primary objective was to enhance the quality of stego images while simplifying the computational complexity associated with modifying four LSB bits to hide confidential data [17,18]. The technique relies on the pixel differences between the original and stego-image pixels. It achieves commendable overall imperceptibility and is applicable to both colored and grayscale

images. The concealment of secret information occurs prior to any pixel value modifications. This approach ensures the preservation of the message while enhancing the quality of the stego-image. The key advantage of utilizing this method over the LSB replacement technique is its ability to generate higher-quality stego-images.

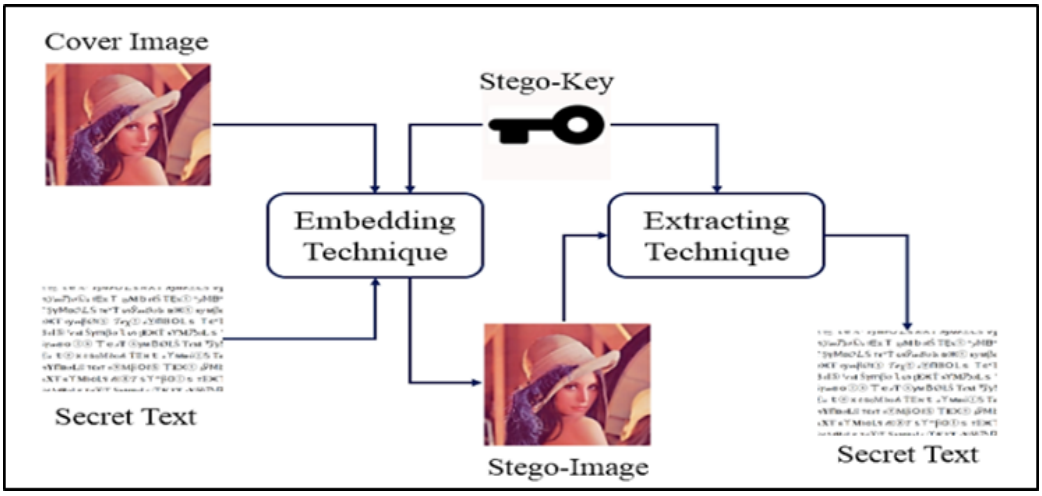

FIGURE 1. LSB mechanism [16].

The PVD technique was originally introduced by Wu and Tsai in their pioneering work [19]. The fundamental idea behind PVD involves quantizing the disparities in neighboring pixel values and then incorporating a concealed message based on the resulting values. This technique organizes a cover image into two successive, non-overlapping pixel blocks following a zig-zag pattern. Moreover, the bit capacity for concealment within each block is established by evaluating the discrepancy between two pixels, which is categorized into several predefined intervals [20]. The choice of these intervals in a range table is influenced by the sensitivity of the human visual system. By default, this method employs data from two horizontally adjacent pixels to gauge the difference. PVD offers enhanced capacity and resilience against RS analysis attacks, making it more secure than LSB. To thwart RS detection attacks, the peak signal-to-noise ratio (PSNR) must exceed 40dB, which is considered good in terms of visual quality. It's worth noting that no steganography technique currently exists that can withstand all steganalysis attempts. PVD typically excels in imperceptibility when compared to LSB, as measured by Human Visual System (HVS) evaluation tools like SSIM. However, PVD is susceptible to pixel difference histogram (PDH) attacks. To enhance security, imperceptibility, and payload, various techniques, including the modulus function (MF), have been incorporated into the development of PVD [21].

III. MATERIAL AND METHOD

To commence the procedure, the initial step involves uploading a pre-prepared cover image in PNG, JPG, or BMP format. Subsequently, employing the initial method, a stego-image is generated, and the hidden text is embedded within the cover image. Subsequently, the stego-image is generated, and its durability, capacity, and imperceptibility are evaluated by computing and closely examining the PSNR and MSE measurements. The process is iterated using grayscale images and the subsequent image algorithm. The experiment is centered on images with dimensions of 1024 x 1024.

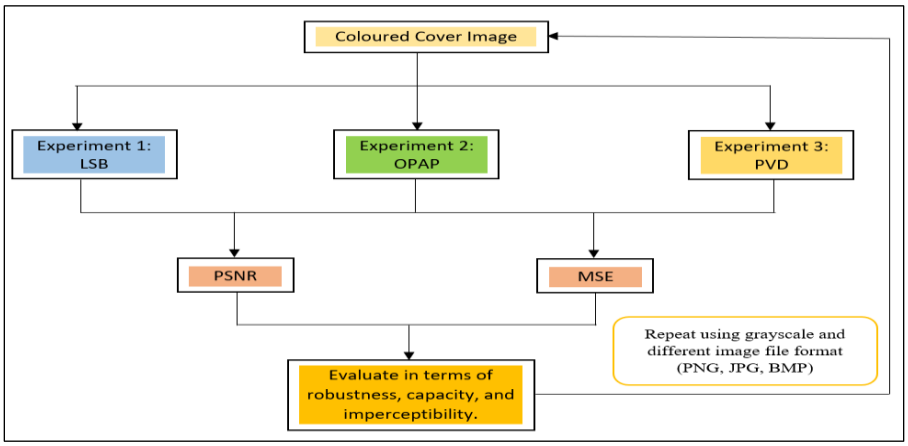

FIGURE 2. Overall structure of experiment.

1. DATA COLLECTION

In this experiment, the research employs three (3) distinct picture formats as cover images. The cover material consists of four standard pictures, specifically Lena, Tiffany, Baboon, and Peppers, each with pixel dimensions of 1024 x 1024. These images are utilized as cover images in both grayscale and color throughout the testing phase. The dataset was sourced from the USC SIPI Volume 3: Miscellaneous website (https://sipi.usc.edu/database/database.php?volume=misc). This dataset is primarily utilized for steganographic techniques, emphasizing imperceptibility and payload capacity.

FIGURE 3. Host images.

2. PERFORMANCE MEASURES

This experiment concentrates on imperceptibility, embedding capacity, robustness, and security. Nevertheless, the literature has proposed several methods for evaluating the efficacy of steganographic methods.

Various methods can be employed to assess whether the quality of an image remains unaffected after embedding a steganographic message. One straightforward approach is to compute the Euclidean Distance between every pixel of the two pictures. Recent research has also explored alternative metrics, such as the Image Quality Index, Structural Similarity Image Quality Assessment (SSIM), Image Fidelity, and the Mean Difference.

The term “payload capacity” refers to the size of the hidden message that can be accommodated within the cover image. A larger payload capacity enhances the efficiency of the steganography method, as it

requires fewer cover images to convey messages. However, it's important to note that an increase in payload size tends to have greater impact on the imperceptibility factor [24].

Security is assessing the ability to evade detection, which involves extracting information from the image to determine if it conceals data, is crucial.

After the text has been integrated, imperceptibility is employed to measure the extent of distortion imposed on the cover image. Excessive distortion can adversely affect the image quality, potentially becoming noticeable to the human eye.

The phrase "robustness" refers to an image's capacity to preserve concealed text even in the face of multiple image-modification operations, such as sharpening, blurring, introduction of noise, cropping, and sharpening [22]. In essence, robustness signifies the algorithm's capability to safeguard the information concealed within the cover medium, even when significant alterations are applied to the cover [23]. It also pertains to the amount of data that can be hidden without compromising or erasing the existing data [24]. Elevated PSNR values play a crucial role in reducing the risk of secret data exposure, a critical factor when encrypting important messages within images.

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.

1.1 Peak Signal-to-Noise Ratio (PSNR)

The PSNR magnitude is commonly employed to evaluate the degree of distortion introduced to a cover image during data concealment [12]. PSNR, which stands for Peak Signal-to-Noise Ratio, measures the maximum signal-to-noise ratio caused by distortion and is typically expressed in decibels (dB). A robust PSNR rating exceeds 40 dB, but the acceptable range falls between 30 and 40 dB. A higher PSNR value indicates superior image quality [25]. It is important to emphasize that the PSNR value is solely derived from the Mean Squared Error (MSE) value.

1.2 Mean Square Error (MSE)

The MSE value, as described in [12], is derived from the mean square of the distinctions between pixels in the actual and stego images. It quantifies the degree of distortion introduced by the data concealment method on the cover image. It is desirable for the MSE to be minimized, as there is an inverse relationship between accuracy and the MSE value. When the genuine and stego images are identical, the MSE value is 0.

IV. DATA ANALYSIS

The research study utilized three algorithms (LSB, OPAP, and LSB) and employed three different picture file formats (BMP, PNG, and JPG), all with cover images sized at 1024 x 1024 pixels, presented in both color and grayscale variations. This segment will present and deliberate upon the obtained results. Notably, MATLAB was employed to execute the LSB and PVD algorithms, while OPAP was implemented in Google Colaboratory. The findings are visualized through graphical representations.

1. OUTPUT FOR PSNR AND MSE OF COLOURED IMAGES

In this subsection, we delve into the experimental outcomes obtained from the three algorithms: LSB, OPAP, and PVD, all applied to colored images with a pixel size of 1024 by 1024. Figures below illustrate the average results for PSNR and MSE, respectively, across different algorithms and picture file formats (BMP, PNG, JPG).

The three bars in under each algorithm in the bar chart represent colour stream Red, Green, Blue (RGB). According to figure below, the OPAP algorithm demonstrates the highest PSNR, followed by the LSB and PVD algorithms. In terms of picture formats, PNG exhibits the highest PSNR value, outperforming BMP and JPG. Figure 5 represents the PSNR values of OPAP, LSB, and PVD in percentage in a straightforward point of view. In contrast, Figure 6 reveals that the MSE for the OPAP algorithm is the lowest, as expected when compared to LSB and PVD. Conversely, the JPG format exhibits the lowest MSE values, while the differences between PNG and BMP are not substantial.

Taking both PSNR and MSE values into consideration, it can be inferred that the OPAP algorithm boasts the highest PSNR and the lowest MSE. This indirectly suggests that OPAP is the most proficient algorithm among LSB and PVD.

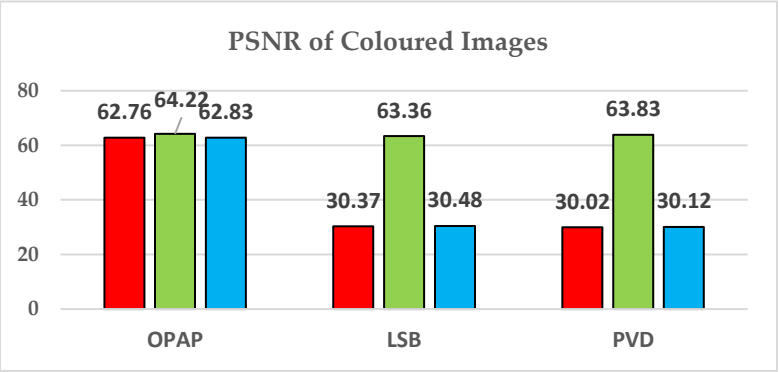

FIGURE 4. PSNR of coloured images based on image formats.

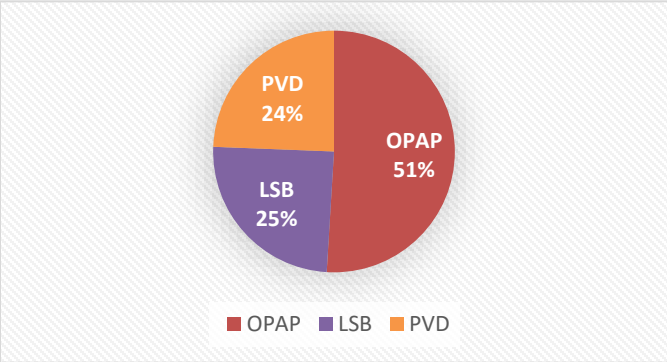

FIGURE 5. PSNR representation chart.

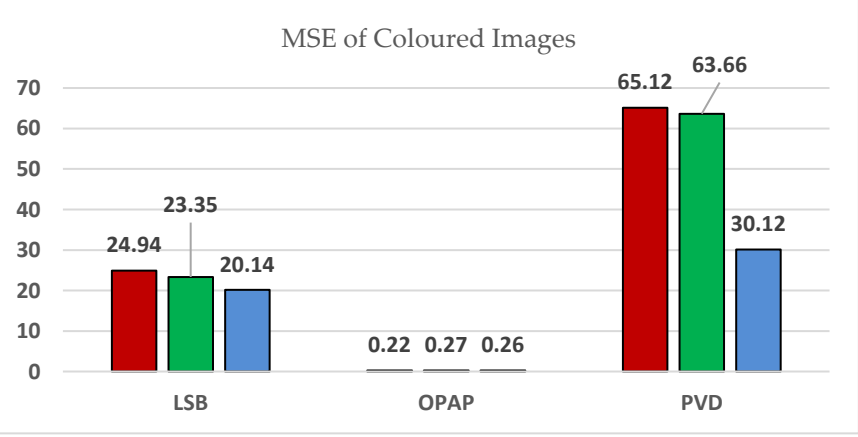

FIGURE 6. MSE of coloured images based on image formats.

2. COLOURED VERSUS GRAYSCALE IMAGES

In this section, we present and analyze a comparative assessment of PSNR and MSE between colored and grayscale images. As illustrated in Figure 7 below, both colored and grayscale images exhibit relatively high PSNR values. Consequently, our focus shifts to the MSE values, which reflect the divergence between the stego image and the original standard image.

In this context, grayscale images outperform colored images, primarily owing to their superior picture quality and lower MSE values when compared to their colored counterparts.

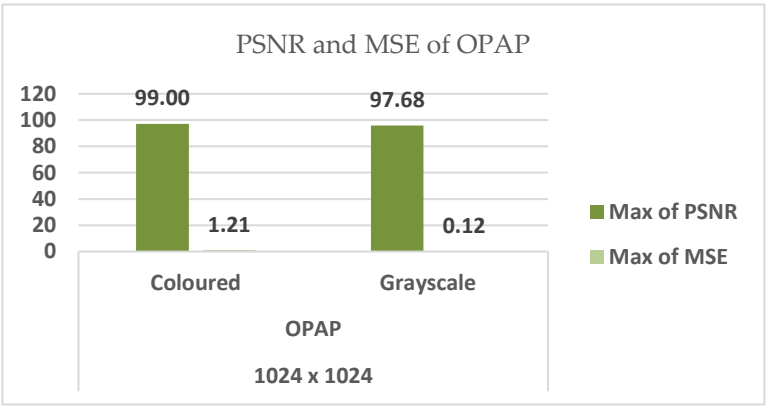

FIGURE 7. Comparison of PSNR and MSE of OPAP.

Colored and grayscale images exhibit distinctions in various aspects, and these dissimilarities result in divergent outcomes when text is embedded. Colored images encompass multiple channels of color information, encompassing red, green, and blue (RGB). In contrast, grayscale images typically possess a solitary intensity channel. Color images offer a broader spectrum of detail and visual information, often boasting enhanced visual appeal. Conversely, grayscale images find utility in specific applications where color isn't essential, such as in medical imaging.

Additionally, it is indicated that the G channel displays a stronger correlation with both the R and B channels than the correlation between R and B. Consequently, aligning the modification directions of the R and B channels with those of the G channel enhances resistance to detection. The color channels are interdependent, meaning that even a minor alteration to the image can result in a significant impact. As depicted in Figure 7, the disparities between colored and grayscale images are not substantial when considering PSNR and MSE. Both colored and grayscale images exhibit PSNR values that exceed the threshold for good image quality. However, when it comes to MSE values, grayscale images outperform colored ones due to their single-channel intensity nature. Consequently, grayscale images are superior to colored images in terms of quality.

3. OUTPUT OF OPAP GRAYSCALE IMAGES

In this section, we are conducting a comparison of the results achieved with the OPAP algorithm, specifically focusing on its performance with grayscale images. This choice is based on the established superiority of grayscale images over colored ones in terms of minimizing the differences between the original and stego images. The outcomes are presented across different image file formats, namely BMP, JPG, and PNG, with the aim of identifying the most suitable and compatible image format for use.

As depicted in Figure 8 below, it becomes evident that JPG produces stego images of lower quality, leaving BMP and PNG as the remaining options. Among these, when considering the four images, three PNG images exhibit relatively higher PSNR values compared to BMP. While BMP boasts competitive values when compared to PNG, it is PNG that stands out as the most suitable choice for producing the highest quality stego images.

Figure 9, presented below, showcases the resulting PNG stego images generated using the OPAP algorithm in both colored and grayscale formats. Upon examination, these output images appear quite similar to the original ones, exhibiting minimal distortion and impressive image quality.

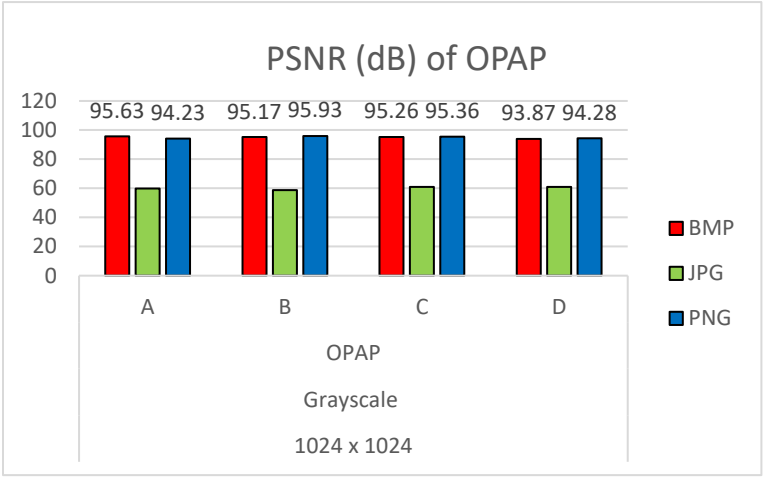

FIGURE 8. PSNR of grayscale images based on image formats.

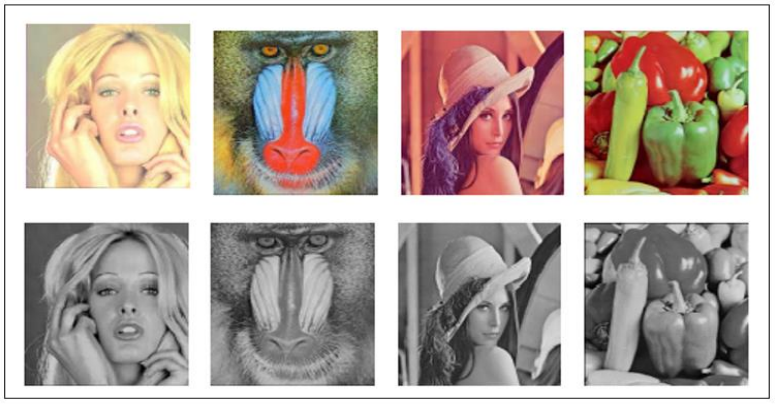

FIGURE 9. OPAP stego-images.

V. DISCUSSION

Based on the experiment, it is concluded that among the three algorithms, OPAP has a better capability to produce a quality stego-image. Moreover, in order to produce an enhanced quality stego-image with higher robustness, imperceptibility, and security, OPAP can be innovated with Knight's Tour (KT). For increased image security, KT and OPAP are used in conjuction with a random point, resulting in the cutting-edge Differentiation Random Point Factor (DRPF). This new algorithm can be utilized to integrate confidential bits into the pixels of compressed images. The integration of KT and OPAP algorithms with DRPF is anticipated to produce steganographic images characterized by exceptional security, robustness, and higher imperceptibility.

VI. CONCLUSION

The assessment of the impact on image quality and information loss caused by the implemented processes in the suggested image steganography approach was conducted using various evaluation techniques. The evaluation methods for the stego image can be categorized as objective or subjective. Objective methods involve identifying differences through numerical criteria and employing various measures, such as ground

truth or statistical knowledge. In contrast, subjective methods rely on human observation and judgment without specific criteria. In this study, standard evaluation metrics (objective methods) were employed to validate the experiment. These metrics include mean square error (MSE), embedding capacity (EC), bits per pixel (BPP), and peak signal-to-noise ratio (PSNR).

In summary, the spatial domain stands out as a promising foundation for an advanced and effective image steganographic algorithm, thanks to its straightforward yet highly efficient approach. It has the capability to generate high-quality stego images with both substantial embedding capacity and imperceptibility, as evidenced by achieving a high PSNR and low MSE. The comparative experiment conducted leads to the conclusion that OPAP surpasses both LSB and PVD as the superior algorithm. OPAP excels in providing highly secure stego images, boasting PSNR and MSE values of 64.22 and 0.27, respectively.

The work on enhancing steganography systems is an ongoing endeavor, and it has unveiled several promising directions for future exploration. For instance, there is potential in merging the spatial domain with the frequency domain, along with the utilization of methodologies like machine learning and deep learning, to bolster security. This approach has the potential to enhance both the security and robustness of the system. Image steganography is a multifaceted field, offering numerous avenues for system improvement. Combining various data hiding techniques, such as watermarking and cryptography, with image steganography could potentially elevate the system's effectiveness and security. One of the primary challenges in steganography technology pertains to expanding the capacity for carrying secret messages, which significantly influences security and robustness. Given the limitations posed by the use of PSNR in this context, it is preferable to preprocess the secret message beforehand and imbue it with dynamic properties through the embedding technique. This collaborative approach integrates the pre-processing stage seamlessly with the concealment process.

REFERENCES

1. Abdulazeez, A. M., Hajy, D. M., Zeebaree, D. Q., & Zebari, D. A. (2021). Robust watermarking scheme based LWT and SVD using artificial bee colony optimization. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 1218-1229.
2. Alsandi, N. S. A., Zebari, D. A., Al-Zebari, A., Ahmed, F. Y., Mohammed, M. A., Albahar, M., & Albahr, A. A. (2023). A Multi-Stream Scrambling and DNA Encoding Method Based Image Encryption. *Computer Systems Science & Engineering*, *47*(2).
3. Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.
4. Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2018, October). Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. In *2018 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 312-317). IEEE.
5. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326.
6. Hosmer, C. (2006). Discovering hidden evidence. *Journal of Digital Forensic Practice*, *1*(1), 47-56.
7. Hernandez-Castro, J. C., Blasco-Lopez, I., Estevez-Tapiador, J. M., & Ribagorda-Garnacho, A. (2006). Steganography in games: A general methodology and its application to the game of Go. *computers & security*, *25*(1), 64-71.
8. Zebari, D. A., Haron, H., Zeebaree, D. Q., & Zain, A. M. (2019, August). A simultaneous approach for compression and encryption techniques using deoxyribonucleic acid. In *2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)* (pp. 1-6). IEEE.
9. Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications*, *77*(13), 17333-17373.
10. Chakkaravarthy, S. S., Sangeetha, D., & Vaidehi, V. (2019). A survey on malware analysis and mitigation techniques. *Computer Science Review*, *32*, 1-23.
11. Zebari, N. A., Zebari, D. A., Zeebaree, D. Q., & Saeed, J. N. (2021). Significant features for steganography techniques using deoxyribonucleic acid: a review. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(1), 338-347.
12. Zebari, D. A., Zeebaree, D. Q., Saeed, J. N., Zebari, N. A., & Adel, A. Z. (2020). Image steganography based on swarm intelligence algorithms: A survey. *people*, *7*(8), 9.
13. Gutub, A., & Al-Ghamdi, M. (2019). Image based steganography to facilitate improving counting-based secret sharing. *3D Research*, *10*(1), 6.
14. Neeta, D., Snehal, K., & Jacobs, D. (2006, December). Implementation of LSB steganography and its evaluation for various bits. In *2006 1st international conference on digital information management* (pp. 173-178). IEEE.
15. Kurak Jr, C. W., & McHugh, J. (1992, December). A cautionary note on image downgrading. In *ACSAC* (pp. 153-159).

16. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66.
17. Turitsyna, E. G., & Webb, S. (2005). Simple design of FBG-based VSB filters for ultra-dense WDM transmission. *Electronics letters*, *41*(2), 1.
18. Darabkh, K. A., Al-Dhamari, A. K., & Jafar, I. F. (2017). A new steganographic algorithm based on multi directional PVD and modified LSB. *Information Technology and Control*, *46*(1), 16-36.
19. Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern recognition letters*, *24*(9-10), 1613-1626.
20. Amirtharajan, R., Adharsh, D., Vignesh, V., & Balaguru, R. J. B. (2010). PVD blend with pixel indicator-OPAP composite for high fidelity steganography. *International Journal of Computer Applications*, *7*(9), 31-37.
21. Pradhan, A., Sekhar, K. R., & Swain, G. (2017). Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks. *Security and Communication Networks*, *2017*.
22. Zebari, D., Haron, H., & Zeebaree, S. (2017). Security issues in DNA based on data Hiding: A review. *International Journal of Applied Engineering Research*, *12*(24), 0973-4562.
23. Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2019). Hybrid Robust Image Steganography approach for the secure transmission of biomedical images in Cloud. *EAI Endorsed Transactions on Pervasive Health and Technology*, *5*(18), e1-e1.
24. Zeebaree, D. Q., Abdulazeez, A. M., Hassan, O. M. S., Zebari, D. A., & Saeed, J. N. (2020). Hiding image by using contourlet transform. *vol*, *83*, 16979-16990.
25. Maji, G., & Mandal, S. (2019). Secure and robust image steganography using a reference image as key. *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN*, 2278-3075.