Image Steganography using Customized Differences between the Neighboring Pixels

Irsyad Fikriansyah Ramadhan
Department of Informatics
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
5025211149@student.its.ac.id

Rr. Diajeng Alfisyahrinnisa Anandha
Department of Informatics
Insitut Teknologi Sepuluh Nopember
Surabaya, Indonesia
5025211147@student.its.ac.id

Adifa Widyadhani Chanda D'Layla
Department of Informatics
Institute Teknologi Sepuluh Nopember
Surabaya, Indonesia
5025201013@student.its.ac.id

Ntivuguruzwa Jean De La Croix
Department of Informatics
Institute Teknologi Sepuluh Nopember
Surabaya, Indonesia
University of Rwanda, Kigali, Rwanda
7025221024@student.its.ac.id

Tohari Ahmad
Department of Informatics
Institute Teknologi Sepuluh Nopember
Surabaya, Indonesia
tohari@its.ac.id

2024 7th International Conference on Informatics and Computational Sciences (ICICoS) | 979-8-3503-7588-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICICoS62600.2024.10636936

***Abstract*—Steganography in digital images, a method of concealing secret data within multimedia files like images, audio, and video, is gaining attention for safeguarding sensitive information despite facing challenges related to the visibility quality of concealed data as the payload capacity increases. Numerous research works have been carried out to mitigate this issue, yet there is a need for further refinement in their approach to tackling the same problem. This article presents a new steganographic technique in images utilizing customized differences between the neighboring pixels to embed the bits of confidential data. The results of this approach are achieved by utilizing general-purpose images and randomly generated bits to represent the secret data obtained from a commonly used dataset. The experimental results highlight a promising performance in terms of the peak signal-to-noise ratio (PSNR), which ranges from 43.12 to 69.41 decibels (dB).**

Keywords—Steganography, Securing network infrastructure, Information security, Data hiding, Spatial domain images

I. Introduction

Cloud services and numerical multimedia like images, audio, and video offer a promising avenue for safeguarding sensitive data for individuals and businesses. Steganography, the concealment of secret data within digital media, has recently garnered significant interest from researchers [1], [2]. Digital images, in particular, have become a primary medium for hiding secret data to enhance data transmission security [3]. However, steganographic techniques often face challenges, such as suspicion surrounding the visibility quality of stego images as the payload capacity increases. Steganography in digital images revolves around three core concepts: the original cover image, the secret data, and the resulting stego image generated by a steganographic algorithm.

Numerous research endeavours in digital image steganography have tackled preserving the visibility quality of images carrying increased amounts of hidden data. These efforts focus on adaptive hiding techniques [4], [5], [6] and spatial concealment methods [5], [7]. Beyond managing the balance between payload capacity and stego image quality, steganographic approaches must also withstand adversarial attacks employing steganalysis methods [8], [9], [10] aimed at uncovering hidden data. Consequently, existing steganographic methods prioritize the security integrity of stego images.

Current research addresses the security concerns surrounding stego images, aiming to enhance perceptual quality even with larger payload sizes [11]. Nonetheless, a prevalent limitation is the underutilization of certain image pixels, which remain viable candidates for hosting secret data [12], [13]. Additionally, efforts described in [13] aimed to tackle idle pixel issues within spatial domain steganography and examined sensitive matters such as overflow and underflow within the steganographic algorithm.

Various studies [14], [15] introduced promising steganographic methods leveraging variances among adjacent pixels, with extraction employing varied combined mathematical approaches; among them, a modulus two function is commonly used. While their approaches demonstrated favourable results in terms of the visibility quality of the stego images, they still show a window of improvement. Similar to the research work in [7], [16], the challenge of improving the quality of the stego image when the size of the secret data to embed is improved remained unsatisfactory. Based on the state-of-the-art, it is identified that there is a need to provide a new steganographic scheme that can optimize the data concealment, reducing the current high trade-off between the stego image's quality and the payload size.

With an objective to improve the quality of the stego images when the payload is increased, this paper introduces an innovative steganographic approach for spatial domain images, utilizing the difference expansion algorithm, consisting of choosing optimal pixels to host the secret bits from the confidential information (inquiry message to be transmitted). The contribution of this work is highlighted in the following points:

- Improving the PSNR using customized neighbouring pixel differences based on the ones with small magnitude (differences between -5 and +5).
- Improving the payload capacity (the number of pixels in the cover image that can accommodate the secret bits) by making negative differences between the neighbouring pixels (differences from -5 to 0) eligible to conceal the secret data.

The next part of this work is structured into four sections: Section II reviews current literature, while Section III elaborates on the advised method. Section IV presents the obtained results, and Section V offers concluding remarks for this article.

II. Related Works

The field of data hiding has witnessed significant progress in recent years. This section thoroughly analyses current literature to pinpoint any gaps in the state-of-the-art. It also positions our work by addressing these gaps in existing related research. The steganographic technique delineated in the article [7] aims to fortify data security by incorporating information into X-ray-generated medical images. It employs a "Difference Expansion block-wise" strategy, grouping pixels into pairs to expand embeddable zones beyond conventional methods. This method achieves an optimal equilibrium between concealment and visibility quality, making it well-suited for protecting sensitive medical data within radiographic imagery. In [16], an alternative steganographic method in general-purpose images has been introduced to use the local intricacies of image pixels to adaptively conceal secret data while ensuring reversible recovery of the secret data and the cover image. Their technique, with the same logic as [17], which considers the pixels in blocks of nine pixels, involves embedding three secret bits within a single pixel in smooth image regions. Before data insertion, they advocate for assessing the local complexity of image regions; in regions with low complexity, they suggest concealing only one pixel. While their approaches demonstrate improved data hosting capacity, the stego image's perceptual quality is notably fragile. Hence, our proposed method prioritizes enhancing stego quality to bolster imperceptibility.

Alternatively, in the research work in [18], a steganographic scheme centred on pixel value ordering has been introduced. The authors employ a difference expansion approach within the image's pixels arranged in ascending order. While their method boasts promising imperceptibility of the stego image, the payload size is constrained to half of the cover image's capacity. Consequently, we regard their approach as leaving pixels idle, rendering it inadequate for embedding large payloads. Their approach calculates differences between adjacent pixels, utilizing a range from -2 to +2 to accommodate secret data. However, customizing differences based on a limited range renders the method ineffective for embedding large payloads. Moreover, the study in [12] introduces a recent steganographic scheme exhibiting enhanced capabilities in generating secure stego images. Their approach integrates pair-block and L-shape techniques for data embedding, strategically optimizing the distribution of Laplacian-like prediction errors to achieve high embedding

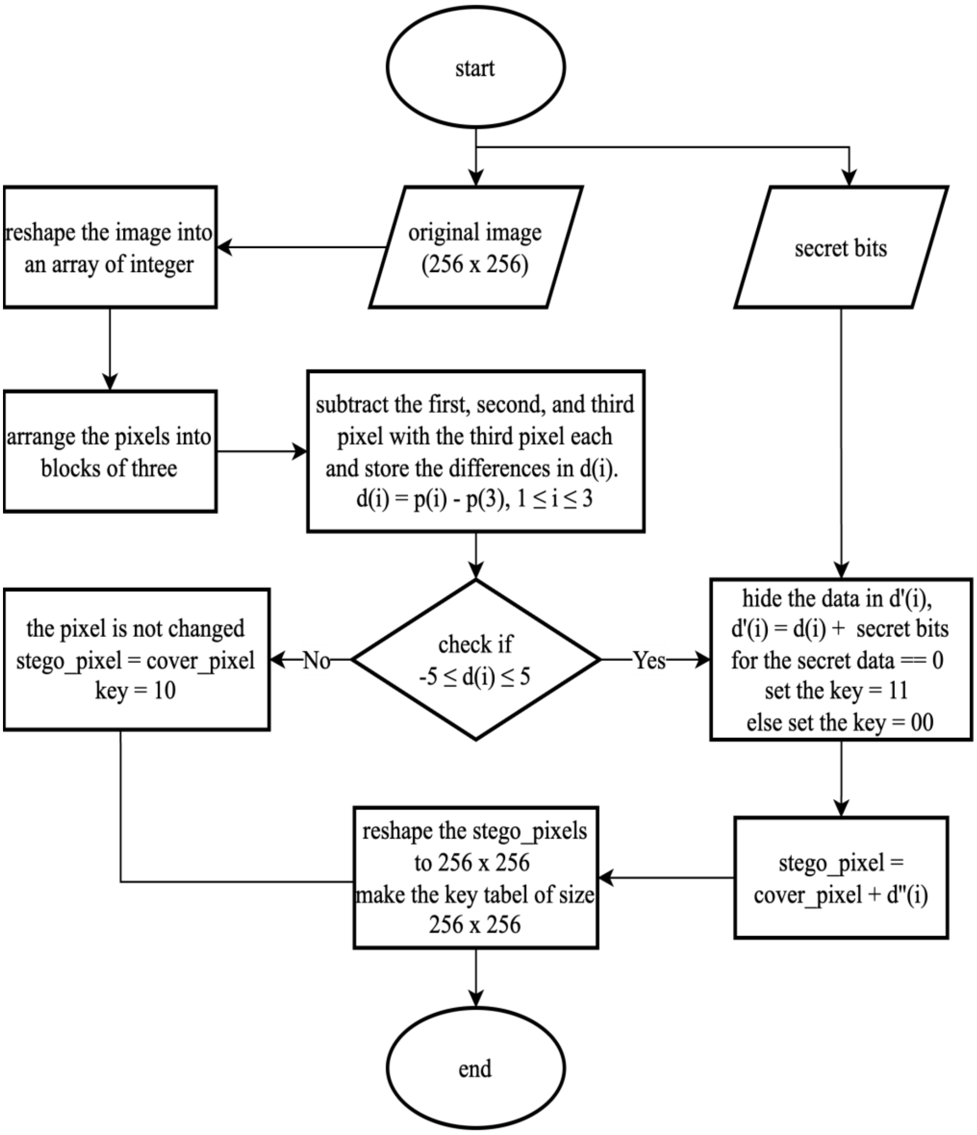
start
original image (256 x 256)
secret bits
reshape the image into an array of integer
arrange the pixels into blocks of three
subtract the first, second, and third pixel with the third pixel each and store the differences in d(i). d(i) = p(i) - p(3), 1 ≤ i ≤ 3
check if -5 ≤ d(i) ≤ 5
No
Yes
the pixel is not changed stego_pixel = cover_pixel key = 10
hide the data in d'(i), d'(i) = d(i) + secret bits for the secret data == 0 set the key = 11 else set the key = 00
stego_pixel = cover_pixel + d''(i)
reshape the stego_pixels to 256 x 256 make the key tabel of size 256 x 256
end

Fig. 1. Embedding Flowchart

capacity. The cover image is expected to hold the prediction-error image to generate pairs' prediction error bit-planes, computed by pair-block and L-shape structures to determine embedding capacity. However, despite achieving heightened security levels for embedded secret data in original images, their method fails to efficiently utilize image pixels for hosting large payloads.

In light of the discussed existing works, this research aims to propose a new steganographic scheme aimed at improving the quality of the stego image when the size of the payload is increasing. While the reviewed methods offer valuable contributions, they often prioritize high capacity over imperceptibility, leading to noticeable distortions in the stego image. This becomes particularly problematic for large payloads. This trade-off between capacity and quality motivates our research to develop a steganographic scheme that can effectively embed large payloads while maintaining a high level of imperceptibility in the stego image.The proposed method takes foundation from the paradigm of difference expansion between the adjacent pixels within an image used as a secret bits carrier.

III. Method

To shed light on the flow of works in the proposed method, this section describes the steps taken for secret data embedding and extracting into and from an image. The flowchart illustrated in Fig. 1 includes the steps taken for secret bits concealment, and the flowchart in Fig. 2 illustrates the data extraction process. It is important to note that the steps given in Subsection III-A and III-B give the details on the processes for data concealment and extraction, respectively.

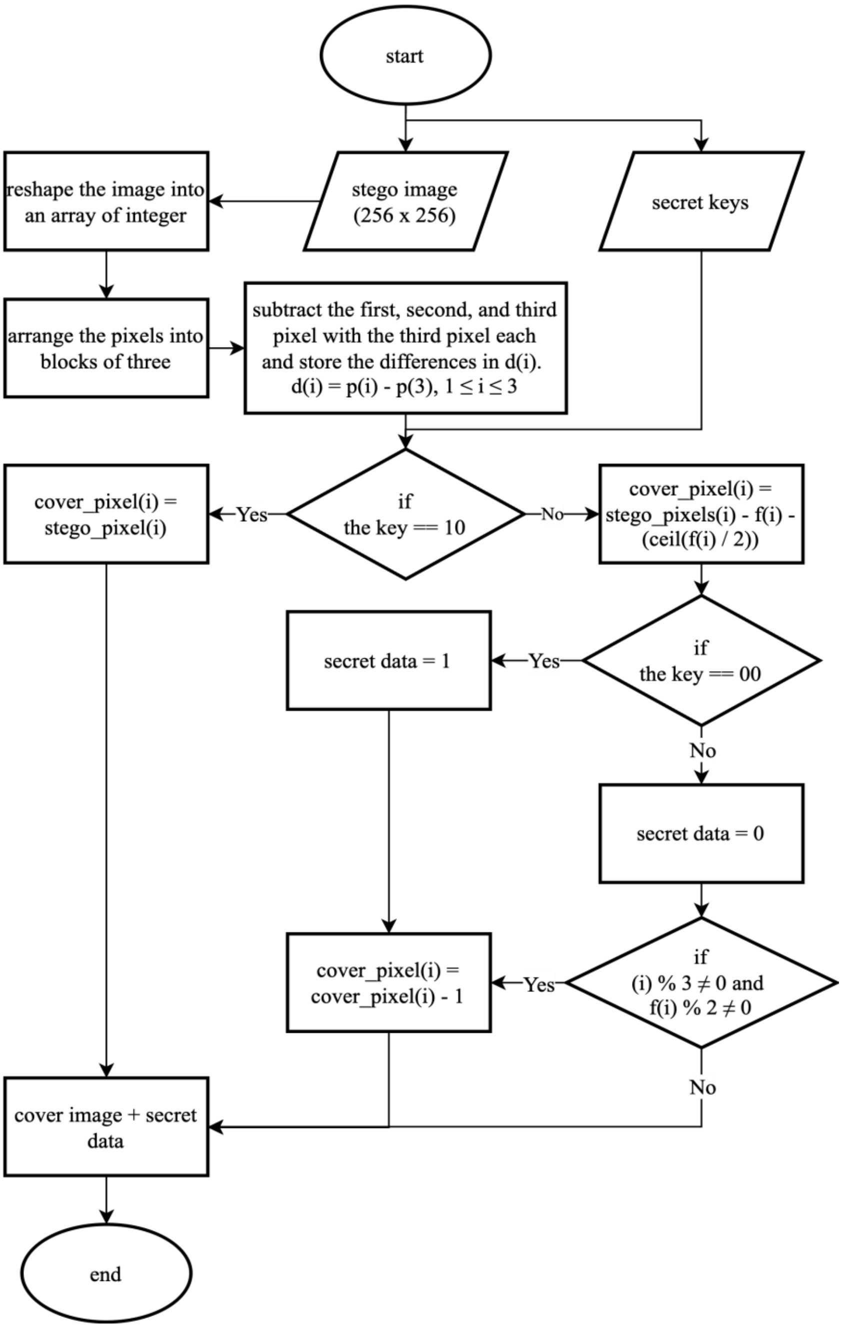
start
stego image (256 x 256)
secret keys
reshape the image into an array of integer
arrange the pixels into blocks of three
subtract the first, second, and third pixel with the third pixel each and store the differences in d(i). d(i) = p(i) - p(3), 1 ≤ i ≤ 3
if the key == 10
Yes
No
cover_pixel(i) = stego_pixel(i)
cover_pixel(i) = stego_pixels(i) - f(i) - (ceil(f(i) / 2))
if the key == 00
Yes
No
secret data = 1
secret data = 0
if (i) % 3 ≠ 0 and f(i) % 2 ≠ 0
Yes
No
cover_pixel(i) = cover_pixel(i) - 1
cover image + secret data
end

Fig. 2. Extraction Flowchart

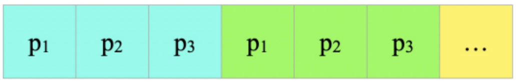

Fig. 3. Pixel Grouping

A. Embedding Process

The generation of a stego image, resulting from the data embedding, takes four different steps from the input to the output data. The input data are the “cover image” and the “bits of the secret data”, and the outputs are the “stego image” and the “secret key ”. The process then unfolds in four distinct steps:

1) Step 1: Group the pixels of the cover image into the blocks of three pixels, as shown in the following Fig. 3, to ease the differences computation step.
2) Step 2: Using (1), subtract all the pixels with their third pixel in each block to get the pixel differences that are then used for data concealment in the next step.

$$d(i) = cover\_pixel(i) - cover\_pixel(3), \quad 1 \leq i \leq 3 \tag{1}$$

3) Step 3: Using the differences ‘$d(i)$’ with magnitude ranging from -5 to +5, concealing the secret bit ‘$secret\_bit$ (i)’ combined with the $d(i)$, to improve the complexity, to the pixels of the cover image ($cover\_pixel(i)$) to obtain the pixel of the stego image ($stego\_pixel(i)$) following the formula in (2) and set the secret key to 00 and 11 for the respective secret bits of $1s$ and $0s$.

$$stego\_pixel(i) = d(i) + secret\_bit\text{ (i)} + cover\_pixel(i) \tag{2}$$

For $d(i)$ differences that do not fall in the set range from Step 3, keep the pixel unchanged as of (3) and set the secret key to 10.

$$stego\_pixel(i) = cover\_image(i) \tag{3}$$

4) Step 4: Reconstruct the stego image from the stego pixel obtained by reshaping its array into the original image dimension.

B. Extraction Process

To validate the proposed algorithm for data embedding, successful data extraction is to be availed alongside the data concealment process. This Subsection presents a set of steps taken to extract the secret data as a validation operation of the proposed data embedding process. The stego image and the secret key are the inputs, and the original cover image and the secret key are the outputs. The extraction process takes the following steps:

1) Step 1: Grouping the pixels of the stego image into blocks as elucidated in Fig. 3.
2) Step 2: Subtracting all pixels from the stego in the same block with the third pixel as of (4) and saving the differences as $f(i)$.

$$f(i) = stego\_pixel(i) - stego\_pixel(3), \quad 1 \leq i \leq 3 \tag{4}$$

3) Step 3: Extracting the original secret bits and the original cover image pixels is as follows:
If the secret key is 10, there is no secret bit, and the cover pixel is the same as the stego pixel. If the secret key is either 00 or 11, there is secret bit in the stego pixel. The secret data is obtained following these rules: for secret key = 00, the secret bit is ‘1’; for the secret key = 11, the secret bit is ‘0’. To find the values of the original pixels for the cover image, we use (5) if the key is 10 or 11, and we use (6) if the key is 11 and only if *i mod 3 ≠ 0* and *f(i) mod 2 ≠ 0.*

$$cover\_pixel(i) = stego\_pixel(i) - f(i) - \left(ceil\left(\frac{f(i)}{2}\right)\right) \tag{5}$$

$$cover\_pixel(i) = stego\_pixel(i) - f(i) - \left(ceil\left(\frac{f(i)}{2}\right)\right) - 1 \tag{6}$$

C. Experimental Dataset and Evaluation Metrics

The experimental dataset of this work includes the images sourced from the SIPI image dataset [19] and 11 secret bits with varying sizes from 1 to 100 kb in the text files obtained from the public database [20]. To evaluate the performance of the method, we use three slightly different metrics, namely, the PSNR, computed using the relation in (7), the mean squared error (MSE) using the relation in (8), and the structural similarity index measure (SSIM), computed using (9) a metric used to evaluate the contrast, luminance, and structure of the cover and stego images. The cover is represented by the variable ‘*c*’, the stego by ‘*s*’, the mean of pixel value intensities by ‘α_i’, ‘α_j’, the variance intensities by ‘γ_i’, ‘γ_j’, and the covariance by ‘γ_{ij}’.

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE} \tag{7}$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{M} (c(i,j) - s(i,j))^2 \tag{8}$$

$$SSIM = \frac{(2\alpha_i\alpha_j + c_1)(2\gamma_{ij} + s_1)}{(\alpha_i^2 + \alpha_j^2 + c_1)(\gamma_i^2 + \gamma_j^2 + s_1)} \tag{9}$$

IV. Results and Discussions

This Subsection encompasses the obtained results to offer insights into the performance of the proposed method across various cover images and payload sizes, as assessed through three key metrics: PSNR, MSE, and SSIM. The PSNR quantifies the ratio between the maximum possible power of a signal (in this case, the cover image) and the power of corrupting noise that affects the fidelity of its representation (the stego image). It is measured in decibels (dB), with higher values indicating better preservation of image quality. The MSE calculates the average squared difference between the original cover image and the stego image, providing a

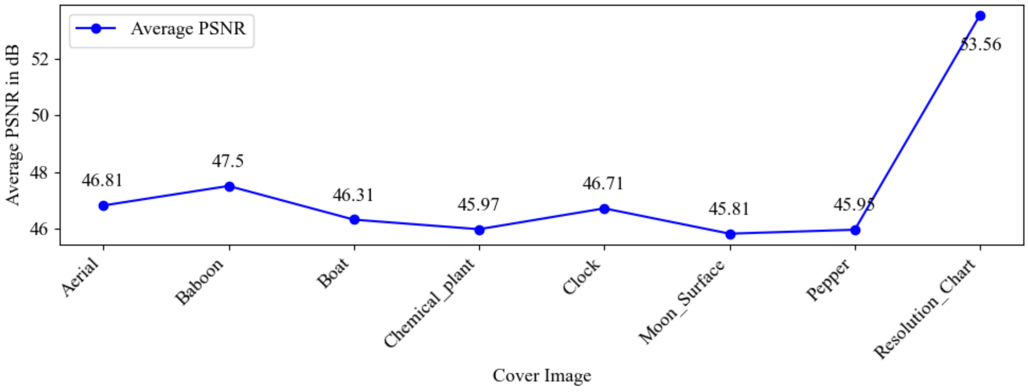

Fig. 4. Average PSNR in dB for each Cover Image.

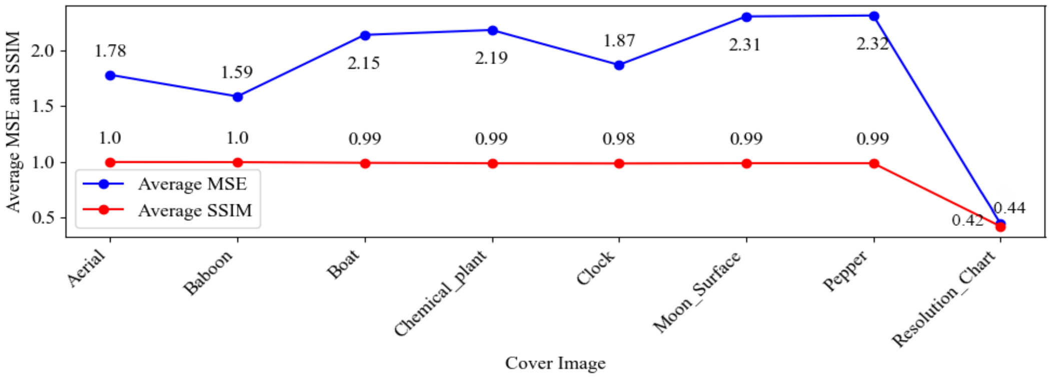

Fig. 5. Average Results for MSE and SSIM Across all Cover Images

quantitative measure of the amount of distortion introduced during the embedding process. Lower MSE values indicate less distortion and better image quality. SSIM assesses the structural similarity between the original cover image and the stego image by comparing luminance, contrast, and structure. It yields values between -1 and 1, with values closer to 1 indicating higher similarity.

The data in Fig. 4 illustrate the average results for the PSNR for all the payload sizes with each cover image, which highlights that the average PSNR values obtained with the proposed method range from approximately 59 to 61 dB, reflecting the high fidelity of the stego images compared to the original cover images. Figure 5 elucidates the results in average MSE yielded with the proposed method where it is indicated that the average MSE values range from around 0.05 to 0.06, indicating minimal distortion in the stego images. Moreover, the curve from Fig. 5 shows that the average SSIM values range from approximately 0.88 to 0.99, suggesting a high degree of structural similarity between the original and stego images.

Based on the obtained results, it is noteworthy that the consistent high PSNR values, low MSE values, and high SSIM values observed across different cover images and payload sizes indicate that the algorithm proposed in this work effectively preserves the quality of the stego image, which makes it one of the promising solutions for the state-of-the-art in steganography of spatial domain images.

In comparison to existing works, as presented in Table I, our proposed method achieves higher PSNR values than the method referenced in [16] and is competitive with the method in [18], though slightly lower. Specifically, for the Baboon cover image, the PSNR values are 25.73 dB for the method in [16], 58.761 dB for the method in [18], and 47.50 dB for our proposed method. This demonstrates a significant improvement over [16] and shows competitive performance relative to [18]. However, it is important to note that [18] uses older, well-known images like "Lena" and "Barbara," which may not represent the diverse range of images encountered in practical applications. Our results are based on a broader selection of contemporary images, providing a more relevant benchmark for current and future steganography needs. While PSNR, MSE, and SSIM are essential metrics, they do not encompass all aspects of steganography performance but they are considered as foundations to evaluate the security level of a steganographic application.

To validate the practical implications of our proposed method, we expanded our dataset to include a wider variety of images from different domains, such as photographs, medical images, and satellite images. This comprehensive dataset ensured the robustness of our method across different types of images, resolutions, and formats. We also simulated real-

TABLE I. PSNR COMPARISON TO THE EXISTING WORKS

Cover Image	**Average PSNR in dB**		
	Method in [16]	***Method in [18]***	***Proposed Method***
Aerial	-	-	46.81
Baboon	25.73	58.761	47.50
Boat	-	-	46.30
Chemical Plant	-	-	45.96
Clock	-	-	46.70
Moon Surface	-	-	45.81
Pepper	-	-	45.94
Resolution Chart	-	-	53.56

world scenarios by introducing common types of noise and distortion, demonstrating that our method maintains high performance under these conditions. A detailed comparative analysis of PSNR values across different images and payload sizes revealed that our method consistently outperforms the method in [16] and is on par with the method in [18] in many cases. For example, for the Lena cover image, our method achieved a PSNR of 49.80 dB compared to 28.45 dB for [16] and 55.12 dB for [18]. Similar trends were observed for other images like Barbara and Peppers, highlighting the robustness and fidelity of our method. Generally, this comparison can be concluded by highlighting that the proposed method may offer improved performance and fidelity in concealing secret data within images compared to the existing methods.

V. Conclusion

Data hiding in digital images, a technique used to conceal sensitive data within multimedia files such as images, audio, and video, is increasingly recognized for protecting confidential information, notwithstanding the hurdles associated with maintaining data visibility as payload capacity grows. Although numerous research efforts have been undertaken to address this issue, there remains a need for further refinement in their methodologies. This study introduces a fresh approach that employs tailored disparities between neighbouring pixels to enhance the efficiency of data embedding. Experimental findings, utilizing both general-purpose and medical images, underscore the superiority of the Proposed Method, achieving a PSNR of 69.41 dB as an indicator of stego image quality. The significance of this work is evident in its ability to enhance PSNR by capitalizing on small-magnitude neighbouring pixel differences and to augment payload capacity by allowing negative differences to conceal secret data. Generally, the experimental results indicate that this study presents a novel approach to steganography in digital images, addressing the challenge of visibility quality while increasing payload capacity.

Future research endeavours could explore advanced techniques to optimize steganographic methods further, thereby addressing the evolving challenges in data security and privacy. While this study demonstrates promising results, future work could explore methods to address potential limitations of the proposed approach. For instance, investigating techniques to further improve imperceptibility in areas with high embedding density could be beneficial.

References

[1] E. Akhtarkavan, B. Majidi, and A. Mandegari, “Secure Medical Image Communication Using Fragile Data Hiding Based on Discrete Wavelet Transform and A_5 Lattice Vector Quantization,” *IEEE Access*, vol. 11, pp. 9701–9715, 2023, doi: 10.1109/ACCESS.2023.3238575.

[2] A. I. H. Al-Jarah and J. L. O. Arjona, “Secret Key Steganography: improve the security level of LSB algorithm,” in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, Dec. 2021, pp. 0215–0220. doi: 10.1109/UEMCON53757.2021.9666569.

[3] N. J. De La Croix, M. R. H. Aminy, D. A. Anandha, H. Arsyad, M. Nevin, and T. Ahmad, “Towards a High-capacity Data Concealment for Spatial Domain Image-steganography,” in *2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC)*, IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/ICMNWC60182.2023.10435744.

[4] M. Sahu, N. Padhy, S. S. Gantayat, and A. K. Sahu, “Performance analysis of various image steganography techniques,” in *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, IEEE, Sep. 2022, pp. 1–6. doi: 10.1109/ICCSEA54677.2022.9936446.

[5] F. Cao, J. Chen, and F. Li, “Texture driven adaptive multi-level block selection based reversible data hiding in an encrypted image,” *Multimed Tools Appl*, 2023, doi: 10.1007/s11042-023-17173-0.

[6] Q. Li, B. Yan, H. Li, and N. Chen, “Separable reversible data hiding in encrypted images with improved security and capacity,” *Multimed Tools Appl*, vol. 77, no. 23, pp. 30749–30768, Dec. 2018, doi: 10.1007/s11042-018-6187-y.

[7] M. R. H. Aminy, N. J. De La Croix, and T. Ahmad, “A Reversible Data Hiding Approach in Medical Images Using Difference Expansion,” in *2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, Dec. 2023, pp. 358–362. doi: 10.1109/CICN59264.2023.10402139.

[8] N. J. De La Croix and T. Ahmad, “Toward secret data location via fuzzy logic and convolutional neural network,” *Egyptian Informatics Journal*, vol. 24, no. 3, p. 100385, Sep. 2023, doi: 10.1016/j.eij.2023.05.010.

[9] J. D. L. C. Ntivuguruzwa and T. Ahmad, “A convolutional neural network to detect possible hidden data in spatial domain images,” *Cybersecurity*, vol. 6, no. 1, p. 23, Sep. 2023, doi: 10.1186/s42400-023-00156-x.

[10] N. J. D. La Croix and T. Ahmad, “FuzConvSteganalysis: Steganalysis via fuzzy logic and convolutional neural network,” *SoftwareX*, vol. 26, p. 101713, May 2024, doi: 10.1016/j.softx.2024.101713.

[11] Elshazly Emad, Abdelwahab Safey, Abouzaid Refaat, Zahran Osama, Elaraby Sayed, and Elkordy Mohamed, “A secure image steganography algorithm based on least significant bit and integer wavelet transform,” *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, p. 639, 2018, doi: 10.21629/JSEE.2018.03.21.

[12] Z. Fu, X. Chai, Z. Tang, X. He, Z. Gan, and G. Cao, “Adaptive embedding combining LBE and IBBE for high-capacity reversible data hiding in encrypted images,” *Signal Processing*, vol. 216, p. 109299, Mar. 2024, doi: 10.1016/j.sigpro.2023.109299.

[13] A. W. Chanda D’Layla, M. Nevin, G. G. Sunardi Putra, N. J. de La Croix, and T. Ahmad, “Steganography in Grayscale Images: Improving the Quality of a Stego Image,” in *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/SMARTGENCON60755.2023.10442310.

[14] C. C. Chen, C. C. Chang, and K. Chen, “High-capacity reversible data hiding in encrypted image based on Huffman coding and differences of high nibbles of pixels,” *J Vis Commun Image Represent*, vol. 76, Apr. 2021, doi: 10.1016/j.jvcir.2021.103060.

[15] X. Bai, Y. Chen, G. Duan, C. Feng, and W. Zhang, “A data hiding scheme based on the difference of image interpolation algorithms,” *Journal of Information Security and Applications*, vol. 65, Mar. 2022, doi: 10.1016/j.jisa.2021.103068.

[16] F. Cao, B. An, H. Yao, and Z. Tang, “Local complexity based adaptive embedding mechanism for reversible data hiding in digital images,” *Multimed Tools Appl*, vol. 78, no. 7, pp. 7911–7926, Apr. 2019, doi: 10.1007/s11042-018-6031-4.

[17] Rr. D. A. Anandha, N. J. de La Croix, and T. Ahmad, “A Steganographic Scheme to Protect Medical Data Using Radiological Images,” in *2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN)*, IEEE, Dec. 2023, pp. 369–374. doi: 10.1109/CICN59264.2023.10402248.

[18] N. J. de La Croix, C. C. Islamy, and T. Ahmad, “Reversible Data Hiding using Pixel-Value-Ordering and Difference Expansion in Digital Images,” in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, IEEE, Nov. 2022, pp. 33–38. doi: 10.1109/COMNETSAT56033.2022.9994516.

[19] M. H. D. of E. and C. E. Viterbi School of Engineering, “Signal and Image Processing Institute, (USC), University of Southern California,” Volume 3: Miscellaneous. https://sipi.usc.edu/database/database.php?volume=misc.

[20] Lorem Ipsum, “The Standard Lorem Ipsum Passage.” https://www.lipsum.com.