Hiding Secret Data Using Reduced Differences within the Pixels of an Image

1st Nadira Milha Nailul Fath Department of Informatics Institut Teknologi Sepuluh Nopember Surabaya, Indonesia 5025211253@student.its.ac.id

3rd Ntivuguruzwa Jean De La Croix Department of Informatics Institut Teknologi Sepuluh Nopember Surabaya, Indonesia University of Rwanda Kigali, Rwanda 7025221024@student.its.ac.id 2nd Moh. Rosy Haqqy Aminy Department of Informatics Institut Teknologi Sepuluh Nopember Surabaya, Indonesia 5025211012@student.its.ac.id

4th Tohari Ahmad Department of Informatics Institut Teknologi Sepuluh Nopember Surabaya, Indonesia tohari@its.ac.id

Abstract-In the modern era, where vast amounts of data traverse public networks, the risk of data breaches is significant. Steganography, a method of concealing data within digital objects like images, is employed to secure sensitive information during transmission. However, utilizing digital images for this purpose often involves a trade-off between image quality and data quantity. To address this challenge, this study introduces a novel steganographic approach based on adjacent pixel differentiation within digital cover images. By customizing pixel differences, the method identifies optimal embedding locations minimize distortion in the resulting stego image. Experimental results demonstrate an average peak signal-tonoise ratio (PSNR) of 65.97 decibels (dB), indicating high stego image quality. This metric serves as a precise measure of the proposed method's effectiveness, with higher PSNR values denoting superior stego image quality.

Keywords—data protection, digital images, information security, securing network infrastructure, steganography

I. INTRODUCTION

Data hiding in digital information security paradigms is a broad field that encompasses various research areas. "hiding" involves shielding confidential information through hidden communication networks. In this context, cryptography and steganography have received considerable attention in recent years [1]. Steganography, diverging from cryptography, consists of protecting secret data by hiding them in the content digital medium such as audio [2], text [3], video [4], and images [5]. Several steganography algorithms have been developed using digital images as cover media [6], [7]. The use of images is based on the fact that they are considered as pervasive digital objects over the public network. Though various existing works tried to address the general steganography problem, there is still a trade-off between the payload size and the stego image quality, making it a significant problem for the security of the secret data transmitted. The research works in [8] [9] are considered due to their nature to be the most fitting algorithms in line with difference expansion (DE), which is supposed to be one of the most significant steganographic paradigms to yield quality results [10]. Though DE has achieved outstanding results, some flaws remain, like unused pixels in the cover image and distorted stego images.

Besides the challenge of idle pixels for the data embedding eligibility, the previously proposed methods present a drawback of low-quality stego images, making them vulnerable to various attacks, mostly adaptive steganalysis methods [11], [12]. The steganalysis methods mainly target the detection of any hidden data transmission that may result in data alteration during transmission. Furthermore, previous steganographic schemes [13], [14] have faced significant challenges in balancing the quality of the images after data embedding, measured using the peak-signal-to-noise ratio (PSNR) in decibels (dB), with the size of the secret bits to be concealed in the cover image measured in bits per pixel (bpp). This trade-off has not been effectively resolved, preventing cover images from carrying a substantial amount of confidential information ensuring lossless extraction of the secret data and the cover image.

To mitigate the flaws identified in the existing works, this study presents a new steganographic scheme to improve the quality of the stego image when hosting a large amount of secret data. This work considers general-purpose images used in the previously proposed works to make it possible to benchmark the obtained results. The contribution of this study is based on the following highlighted points.

- Optimizing the differences between the neighbouring pixels by selecting the best fits to use them as security enhancement keys because they are combined with the secret data for data embedment.
- Expanding the pixel differences between the adjacent columns strengthens the security of the stego image and improves its quality. It is important to note that all the obtained PSNR values are planned to be consistently superior to 30 dB, a threshold value for imperceptible steganography.

The structure of this article is organized into four main sections. Section II reviews the existing works relevant to this study, focusing on their algorithms and their relationship to this research. Section III details the proposed scheme, explaining its methodology and design. Section IV presents and discusses the results obtained from experiments. Finally,

Section V concludes the study and suggests potential future research directions.

II. EXISTING WORKS

This section discusses the existing works following the main idea of digital image steganography as mathematically presented in (1) and (2). Using (g[.]) as a function to represent the data embedding operation, C_{Image} , Sec_{data} and S_{Image} as the respective variables for the cover image, secret bits, and stego image.

• Data concealment:

$$S_{Image} = g[C_{Image}, Sec_{data}]$$
 (1)

Image and data recovery:

$$(C_{Image}, Sec_{data}) = g^{-1}[S_{Image}]$$
 (2)

Based on the equations above, the cover image represents an original used as a carrier of the secret data bits. The hidden bits are the binary representations of the confidential message to be concealed in the cover image, and the stego image is an image resulting from a combination of the secret data and the cover image through an embedding algorithm (EA). The embedding algorithm represents an algorithm that hides the secret data in the pixels of the cover image. Based on the fact that hiding the data is valid if the receiver can extract the hidden data[15], the formula in (2) shows how to extract the secret data and the original cover image using the stego image as an input object.

The study in [16] proposed a novel steganography algorithm based on difference expansion (DE) by grouping the pixels in a fashion of triplets. In their method, they used the differences between the pixels of the identical triplet to embed the secret data. Their method's novelty was set to reside on the use of a minimal pixel of the triplet as a subtractor from other pixels. Under the same umbrella of DE, the researchers in [5] proposed another innovative scheme to improve the data embedment with optimized pixel use. Differently from [16], the work in [5] created a dynamic function used as a subtractor from the transformed secret data, and that difference was then used to conceal the hidden data in the cover image. Though the proposed works in [5] and [16] contributed significantly to the state-of-the-art, the problem of a remarkable trade-off between the payload size and the stego image quality has not been completely mitigated.

Furthermore, drawing from the findings in [17], which presented an innovative method for improving the quality of stego images with higher secret data sizes in standard images, the confidential data transmission can be significantly enhanced. This method uses idle spaces after data encryption to conceal secret information. Using predictors based on linear regression, the study aims to improve accuracy and incorporates a map for error detection, significantly

increasing the data hiding rate and ensuring a successful recovery of the secret data and the cover image.

The research in [10] presents a modern steganographic method with advanced features for creating protected images with hidden secret data. This approach combines pixel blocks in L-fashion approaches to embed the secret data, fine-tuning the arrangement of Laplacian-like forecast inaccuracies to achieve an outperforming capacity for data concealment. The carrier image is meant to contain the prediction-error picture, which is obtained based on the pixel blocks in pairs and L-fashion. Nevertheless, in spite of the superior imperceptibility of the stego image, based on its quality, the method in their study does not efficiently use image pixels to accommodate large payloads. With the same DE paradigm in [18], a different steganographic technique for digital images has been proposed, which leverages the local regions of a cover image to embed the secret data in adaptive ways.

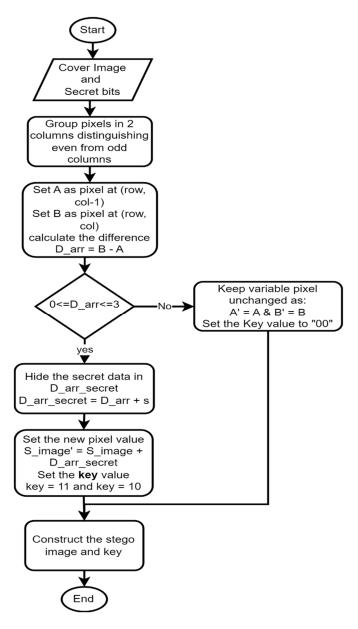


Fig. 1. Illustration of the Embedded Process

Enlightened by the existing works in this section, a new steganography method is proposed based on DE. As detailed in the next section, the proposed method consists of using differences between adjacent pixels customized based on their magnitude for improved results in addressing the steganography problem compared to the existing works.

III. PROPOSED METHOD

This section presents steps taken for data embedding and extraction processes, which are the main parts of the proposed approach. It is crucial to note that the embedding process is considered valid if the extraction process is successful. Figure 1 illustrates a schematic flow of steps for the embedding process, and Fig. 2 elucidates the extraction process portrait. Subsections III. A and III. B explicitly highlight the steps of the Proposed method. The "Embedding process", presented first, involves using adjacent pixels to calculate the differences between neighbouring pixels. This calculation primarily targets pixels with even columns to optimize the embedding capacity within these columns. In line with pixels use optimization, a conditional range is applied to the pixels designated for secret data concealment, restricting them to values between 0 and 3. Upon completion of this data embedding process, a stego image is constructed. The "Extraction process", presented at the second point, begins by identifying even columns within the pixels of the stego image, followed by iterating through the key table values to identify the pixels with the secret data. This key determines whether a binary number of 1 or 0 is indicated, enabling the extraction of the original embedded secret data. Subsequently, the stego image is sorted into even and odd columns, and computations are performed to reveal the pixels of the cover image.

A. Data Embedding

The method proposed in this study to embed the secret data in the pixels of the cover image goes through a number of steps. The embedding process considers the cover image (CI) and the secret bits (S) as inputs and the stego image (SI) with the key matrix (KM) as the outputs. The following are the steps for the embedding process.

- 1) Step 1: Get the CI and S, the inputs of the process.
- 2) Step 2: Generate and arrange an array of pixels of the CI in one dimension.
- 3) Step 3: Calculate the difference values between adjacent pixels by subtracting odd columns from even columns pixel by pixel. The differences are considered as DP. It is important to note that the differences in the pixels in even columns that are inferior to the pixels of the odd columns are considered fixed values (unchangeable pixels).
- 4) Step 4: Use formula (3) to embed S into eligible DPs (it means differences ranging from 0 to 3) and then add the combination of DP and S to the value of the pixels from CI to obtain the updated pixel value for SI. If the pixel value is changed due to the addition of the secret data, update the KM with '10' and '11'. It is crucial to highlight that this work uses '10' when hiding a secret bit equivalent to '0', '11' when embedding the secret bit equivalent to '1', and default values otherwise.

$$SI = CI + DP + S \tag{3}$$

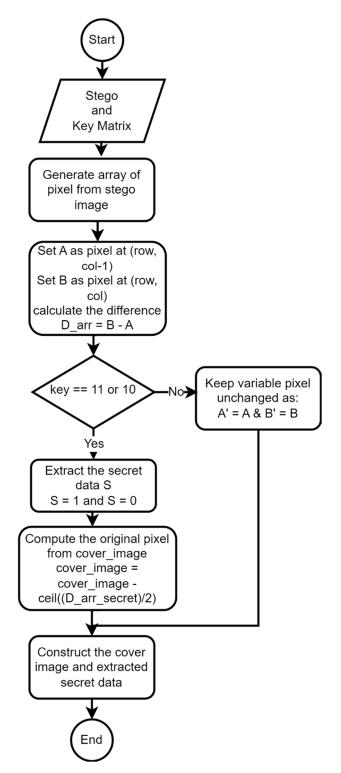


Fig. 2. Flowchart for the Cover Image and Secret Bits Extraction

5) Step 5: Construct SI and KM with new values from Step 4.

B. Secret Data and Cover Image Recovery

The extraction procedure involves a sequence of systematic steps to retrieve the secret data from the SI. The extraction process takes the SI and the KM as inputs and retrieves the S while reconstructing the CI. The following steps outline the extraction process.

1) Step 1: Read the SI and KM as the inputs

- 2) Step 2: Compute the differences between the columns of SI by subtracting the even columns from the odd columns. The calculated differences are stored as DS.
- 3) Step 3: Identify the positions where the secret data is embedded using the values from KM. For each position, extract the secret bit based on the DS. If the KM value is equal to '11', extract '1' as the secret bit, and if the KM value is equal to '10', obtain '0' as the secret bit. The CI is obtained following (4) for KM value equal to '11' or '10' and (5) otherwise.

$$CI = CI - ceil(\frac{DS}{2}) \tag{4}$$

$$CI = SI$$
 (5)

IV. RESULTS AND DISCUSSION

A. Dataset, Experimental Setup and Evaluation Metrics

Cover images from the SIPI dataset [19], a publicly available general-purpose image dataset, have been used in experiments and results generation. Used cover images are the 8 bits of grey-level images taken by seven different cameras with the same characteristics. The secret bits from [20], a publicly available dataset of text files spanning from 1 to 100 kilobits (kb), have been used. The choice of the cover images and secret bits to use in the experimentation is based on their general use in most of the previous works. They have been chosen for a couple of reasons, namely, their performance in experiments and finding a benchmark for the obtained results. The experiments are conducted using MatLab R2024a. The hardware specifications for experimentation are as follows: Processor, AMD Ryzen 7 4700U with Radeon Graphics; RAM, 16 GB; in a Windows 11 Home Single Language Edition. To assess the proposed scheme, two evaluation metrics are used, namely, the peak signal-to-noise ratio (PSNR), which depends on the values obtained from the mean squared error (MSE), and a metric to evaluate the similarity level known as SSIM. The MSE, PSNR, and SSIM are respectively computed using the relations (6), (7), and (8). Considering the pixel intensities as an average of π_i , π_j , with their variance as β_i , β_i and their covariance as β_i .

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(C_{Image}(i,j) - S_{Image}(i,j) \right)^2$$
 (6)

$$PSNR = 10 \times (log_{10}255^2 - log_{10}MSE)$$
 (7)

$$SSIM = \frac{(2\pi_i \pi_j + C_{Image_1})(2\beta_{ij} + S_{Image_1})}{(\pi_i^2 + \pi_j^2 + C_{Image_1})(\beta_i^2 + \beta_j^2 + S_{Image_1})}$$
(8)

B. Results

Table I presents the results of the Peak Signal-to-Noise Ratio (PSNR). The results indicate that the initial PSNR values for the cover images are quite high, particularly for images like 'Chest,' 'Head,' and 'Abdominal,' which start with PSNR values around 75 dB when the payload size is 1 kb. This shows that these images have better initial quality and can maintain higher security for the data to be transmitted. It is crucial to note that as the secret data size increases, there is a general decline in PSNR values across all images. For instance, the 'Baboon' image starts at 65.09 PSNR for a 1 kb payload and decreases to 52.94 PSNR for a 100 kb payload. Similarly, the 'Pepper' image starts at 65.27 PSNR for a 1 kb payload and drops to 50.02 PSNR at 100 kb. Based on the fact that the admissible minimum PSNR is 30 dB, the results show that this method always yields admissible results for a quality stego image. Despite the overall trend of decreasing PSNR with increasing payload size, some images maintain relatively higher PSNR values even at larger payloads. For example, the 'Head' image retains a PSNR of 51.48 even with a 100 kb payload, suggesting it can handle larger data embeddings while still preserving acceptable image quality. These results demonstrate the varying capacity and robustness of different cover images for steganographic purposes.

Furthermore, Table II presents the SSIM results for the same cover images and payload sizes as Table I. The SSIM values, which measure the perceived quality of the stego images compared to the original images, indicate that the

Cove image	Payload size in kb										
	1	10	20	30	40	50	60	70	80	90	100
Baboon	65.09	55.02	52.95	52.93	52.93	52.93	52.92	52.92	52.94	52.94	52.94
Boat	65.11	55.14	52.17	51.05	51.03	51.06	51.04	51.05	51.06	51.05	51.06
Pepper	65.27	55.13	52.17	50.42	50.01	50.01	50.00	50.00	50.04	50.02	50.02
Hand	66.93	61.91	60.09	58.79	57.33	55.55	53.52	52.18	51.55	51.17	51.11
Leg	72.22	62.09	58.81	56.71	53.87	52.64	52.08	51.60	51.06	50.78	50.80
Chest	75.13	64.96	61.33	54.96	53.20	52.13	50.94	50.06	49.92	49.78	49.69
Head	75.41	64.95	61.71	58.97	56.06	53.58	52.06	51.73	51.56	51.48	51.48
Abdominal	75.29	64.93	59.40	53.39	51.87	50.85	50.06	49.66	49.56	49.49	49.49

TABLE II. OBTAINED SSIM RESULTS

TABLE II. OBTAINED COINT RESCETS											
Cove image	Payload size in kb										
	1	10	20	30	40	50	60	70	80	90	100
Baboon	0.999	0.999	0.998	0.998	0.998	0.998	0.998	0.998	0.998	0.998	0.998
Boat	0.999	0.998	0.999	0.996	0.996	0.996	0.996	0.996	0.996	0.996	0.996
Pepper	0.999	0.998	0.996	0.995	0.994	0.994	0.994	0.994	0.994	0.994	0.994
Hand	0.999	0.999	0.999	0.999	0.998	0.998	0.997	0.996	0.996	0.995	0.995
Leg	1.000	0.999	0.999	0.998	0.997	0.996	0.996	0.996	0.995	0.995	0.995
Chest	0.999	0.998	0.997	0.996	0.995	0.994	0.993	0.992	0.991	0.990	0.990
Head	0.999	0.998	0.997	0.996	0.995	0.994	0.993	0.992	0.992	0.991	0.991
Abdominal	0.999	0.998	0.997	0.996	0.995	0.994	0.993	0.992	0.991	0.991	0.991

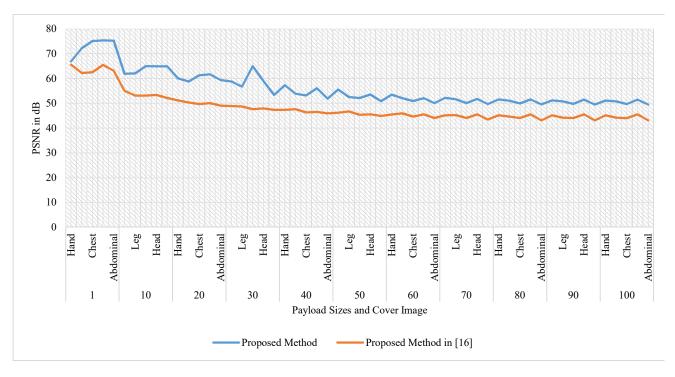


Fig. 3 Comparison of the Obtained to the Existing Reported Results

steganographic method used preserves the visual quality effectively. In this study, all cover images start with SSIM values close to 1.0 when the payload size is 1 kb, reflecting nearly perfect similarity between the original and stego images. As the payload size increases, there is only a slight decline in SSIM values across all images. For instance, the 'Baboon' image maintains an SSIM of 0.998 from 20 kb to 100 kb, while the 'Leg' image shows a minimal reduction from 1.000 at 1 kb to 0.995 at 100 kb. This minor decrease demonstrates the robustness of the method in preserving image quality despite the increased embedded data.

In addition, different images exhibit varying degrees of SSIM reduction, highlighting the varying robustness of different images to data embedding. For example, the 'Chest' image decreases from 0.999 at 1 kb to 0.990 at 100 kb. In contrast, some images, such as 'Hand,' retain higher SSIM values even at larger payloads, with an SSIM of 0.995 at 100 kb. These results illustrate the effectiveness of this study's method in maintaining the structural integrity of cover images, ensuring that the embedded secret data does not significantly compromise image quality.

C. Results Comparison

Comparing different cover images reveals varying degrees of SSIM reduction, which emphasizes the method's adaptability to different types of content. For instance, while the 'Baboon' and 'Leg' images exhibit negligible SSIM reduction even at larger payloads, the 'Chest' image shows a slightly more pronounced decline. Notably, the 'Hand' image stands out for its ability to retain higher SSIM values even at larger payloads, indicating its resilience to data embedding.

Moving on to the comparison with an existing method detailed in [16], Figure 3 illustrates the superior performance of the proposed steganographic method across all considered cover images and payload sizes. Notably, the proposed method consistently maintains higher PSNR values, particularly at larger payload sizes, signifying better

preservation of image quality. For example, the 'Hand' image exhibits a significantly higher PSNR of 51.11 at 100 kb with the proposed method compared to 45.14 with the method outlined in [16]. This improvement is attributed to the optimal use of differences between the adjacent pixels which makes it a more sophisticated embedding techniques designed to minimize distortion while maximizing data hiding capacity. Additionally, the method mitigates any potential degradation caused by data embedding.

Generally, it is identified that the results underscore the superior effectiveness and robustness of the proposed steganographic method in maintaining higher image fidelity while embedding larger amounts of secret data. This superiority is not only evident in the quantitative metrics like SSIM and PSNR but also supported by the method's ability to consistently outperform an existing approach across various cover images and payload sizes.

V. CONCLUSION AND FUTURE SCOPE

This paper proposes a new steganographic algorithm to reduce the effect of a trade-off between the quality of a stego image and the secret bits embedded in the pixels of an image. The foundation of the proposed method is based on the necessity of an improved data-hiding technique to embed a large number of secret bits without the perceptibility of their existence. This research method uses adjacent pixel differentiation within digital images to conceal the bits of the secret message. The embedding process targets even columns of the matrix made of the pixels from a cover image to optimize data concealment, while the extraction process employs a key table generated in the embedding process to retrieve the hidden data accurately. Experimental results demonstrate that the proposed method outperforms existing techniques, underscoring its contribution to the state-of-the-

Future work could enhance this research in several ways. Integrating encryption with steganography would provide

additional security for the hidden data. Assessing the method's robustness against various image processing attacks, such as compression, scaling, and noise addition, is crucial for practical application. Optimizing the algorithm to reduce computational complexity and improve processing speed would increase efficiency.

REFERENCES

- [1] A. I. H. Al-Jarah and J. L. O. Arjona, "Secret Key Steganography: improve 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.
- [2] Moh. M. Amrulloh, T. Ahmad, and N. J. De La Croix, "Analysis of the smoothing and payload distribution method on reversible audio steganography," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, Jul. 2023, pp. 1–5. doi: 10.1109/ICCCNT56998.2023.10307703.
- [3] B. Khosravi, B. Khosravi, B. Khosravi, and K. Nazarkardeh, "A new method for pdf steganography in justified texts," *Journal of Information Security and Applications*, vol. 45, pp. 61–70, Apr. 2019, doi: 10.1016/j.jisa.2019.01.003.
- [4] S. Debnath, R. K. Mohapatra, and R. Dash, "Secret data sharing through coverless video steganography based on bit plane segmentation," *Journal of Information Security and Applications*, vol. 78, p. 103612, Nov. 2023, doi: 10.1016/j.jisa.2023.103612.
- [5] 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.
- [6] B. Pan, T. Qiao, J. Li, Y. Chen, and C. Yang, "Novel Hidden Bit Location Method towards JPEG Steganography," Security and Communication Networks, vol. 2022, 2022, doi: 10.1155/2022/8230263.
- [7] H. Rahman, H. Syarif, D. Wahono, N. J. de La Croix, and T. Ahmad, "A Steganographic Method Based on Pixel Block Differences in Grayscale Images," in 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/SMARTGENCON60755.2023.10442053.
- [8] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, Aug. 2003, doi: 10.1109/TCSVT.2003.815962.

- [9] 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.
- [10] 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, Mar. 2024, doi: 10.1016/j.sigpro.2023.109299.
- [11] N. J. D. La Croix, T. Ahmad, and F. Han, "Enhancing Secret Data Detection Using Convolutional Neural Networks with Fuzzy Edge Detection," *IEEE Access*, pp. 1–1, 2023, doi: 10.1109/ACCESS.2023.3334650.
- [12] N. Jean De La Croix and T. Ahmad, "A Scheme Based on Convolutional Neural Network and Fuzzy Logic to Identify the Location of Possible Secret Data in a Digital Image," *International Journal on Engineering Applications (IREA)*, vol. 12, no. 1, p. 1, Jan. 2024, doi: 10.15866/irea.v12i1.23475.
- [13] A. K. Sahu and A. Gutub, "Improving grayscale steganography to protect personal information disclosure within hotel services," *Multimed Tools Appl*, vol. 81, no. 21, pp. 30663–30683, Sep. 2022, doi: 10.1007/s11042-022-13015-7.
- [14] H. Arsyad, N. J. De La Croix, and T. Ahmad, "A Steganographic Approach to Secure Data Using Pairs-Based Difference Expansion," in 2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, Dec. 2023, pp. 363–368. doi: 10.1109/CICN59264.2023.10402286.
- [15] K. Hu, M. Wang, X. Ma, J. Chen, X. Wang, and X. Wang, "Learning-based image steganography and watermarking: A survey," *Expert Syst Appl*, vol. 249, p. 123715, Sep. 2024, doi: 10.1016/j.eswa.2024.123715.
- [16] M. Meftah Mafazy, J. Terri Agustinus, T. Ikhwanul Haq, N. Jean De La Croix, and T. Ahmad, "Triplets-Based Steganographic Scheme to Improve the Image Quality in Spatial Domain," in 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC), IEEE, Dec. 2023, pp. 1–5. doi: 10.1109/ICMNWC60182.2023.10435875.
- [17] K. Chen and C. C. Chang, "Error-free separable reversible data hiding in encrypted images using linear regression and prediction error map," *Multimed Tools Appl*, vol. 78, no. 22, pp. 31441– 31465, Nov. 2019, doi: 10.1007/s11042-019-07946-x.
- [18] 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.
- [19] "The USC-SIPI Image Database." Accessed: April 15, 2024. [Online]. Available: https://sipi.usc.edu/database.
- [20] "Lorem Ipsum.", www.id.lipsum.com (Accessed April. 15, 2024).