Data Hiding Scheme using Difference Expansion and Modulus Function

Conference Paper · March 2023

DOI: 10.1109/INOCON57975.2023.10100991

Md. Sagar Hossen
Institut Teknologi Sepuluh Nopember
21 PUBLICATIONS **318** CITATIONS

SEE PROFILE

Tohari Ahmad
Institut Teknologi Sepuluh Nopember
148 PUBLICATIONS **1,175** CITATIONS

SEE PROFILE

2023 2nd International Conference for Innovation in Technology (INOCON)
Bangalore, India. Mar 3-5, 2023

Data Hiding Scheme using Difference Expansion and Modulus Function

Md. Sagar Hossen
Department of Informatics
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
Department of Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
6025221064@mhs.its.ac.id

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

Ntivuguruzwa Jean De La Croix
Department of Informatics
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia
African Center of Excellence in Internet of Things
University of Rwanda
Kigali, Rwanda
7025221024@mhs.its.ac.id

2023 2nd International Conference for Innovation in Technology (INOCON) | 979-8-3503-2092-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/INOCON57975.2023.10100991

***Abstract*—Our information is constantly under threat when transmitted through public networks. So, research to keep information secret has been carried out. Mainly, steganography, which consists of hiding data in digital media, receives much attention. Existing steganographic systems identified the need to improve performance by reducing a tradeoff between the peak signal-to-noise ratio (PSNR) and bits per pixel (BPP). In this paper, we propose a new steganographic scheme to embed the bits of secret messages in a digital image's pixels. Our method expands the differences between the neighbouring pixels for secret data concealment. We group the pixels in blocks of size 1×3, and two of the three pixels of the block are candidates to hold the secret bit. We also propose extracting the hidden data to validate our data concealment scheme. To extract the secret data, we also arrange the neighbouring pixels into blocks of three and use their differences, and a modulus function, based on pixels identified carrying the secret data based on the key generated during data concealment. To evaluate the performance of our scheme, we consider the PSNR and the BPP as metrics. The experimental results showed better performance over the existing methods with $68.7790\,dB$ for the PSNR and 0.1562 BPP.**

Keywords—Data hiding, image Steganography, difference expansion, data security, infrastructure

I. Introduction

Private data transmission has been practised for centuries through the public network. Various data security approaches have been proposed to address the problem of unwanted confidential data access, like cryptography, watermarking, and steganography. These approaches' implementation principles and guiding paradigms are different; however, all of them are accounted for as data protection approaches [1]. Among them, steganography is often used, which knew its high application with the increased availability of digital media such as images, audio, and video. Steganography is a data-hiding approach implemented by hiding secret bits of data within digital media content [2]. Although steganography achieved better results in protecting confidential data against unwanted reveals, it has yet to fully attain the level of avoiding suspicion of the digital media carrying secret information. Therefore, different approaches have been proposed [3]–[8] to improve the quality of digital media known as stego. Specifically, the digital image for steganographic payload protection not only provided a high availability in the public network but also showed a drawback of a high tradeoff between the image quality and the payload capacity. When secret data is embedded in a cover image, it changes its pixel values. These changes impact the image's original state; hence, the stego can be easily suspicious. To evaluate the quality of the Stego-image, a standard metric used is PSNR, which reflects the mean squared error (MSE) between the original Cover image and the Stego-image, indicating the imperceptibility of the embedded data [9]. The amount of confidential information in an image is measured in BPP, calculated by dividing the number of secret bits embedded in the image by the total number of pixels as of (1).

$$BPP = \frac{Number\ of\ secret\ bits\ embedded}{Total\ pixels\ in\ the\ cover\ image} \tag{1}$$

In line with digital image steganography, research has been carried out to reduce the tradeoff between the PSNR and the BPP. However, the existing approaches' performance still needs to be improved in both the stego visibility quality with increased payload. Of the existing approaches, pixel value manipulation (PVM) [10] and pixel value differencing (PVD) [11] have achieved significant results in both the PSNR and the payload capacity. Nevertheless, there is a need to maximize the security of the confidential data in the stego images by increasing the yield in the stego visibility when the payload increases.

In this work, we propose a new DE approach combining to enhance the PSNR and increase the steganographic payload with the following contributions:

- Splitting an inquiry image into blocks of three pixels and calculating for embeddable pixels with overlaps that were not used in the previous works.
- Setting a condition of the pixel's embeddability with a small difference between the neighbouring pixels in the blocks.
- Keeping the neighbouring pixels with high differences unchanged to avoid the distortion of the stego image's quality.

The rest of this work is organized in sections. Section II describes some recent works we have improved, Section III includes the method proposed in this work, Section IV describes the obtained results, and this work is concluded in section V.

II. EXISTING METHOD

In [12], a steganographic scheme to hide data in reduced and expanded differences between adjacent pixels has been proposed with a secret key used to extract the secret message. For a methodology of their work, they arrange the image's pixels in blocks of four pixels with notations h_0, h_1, h_2, and h_3, respectively, for the first, second, third, and fourth pixels and then calculate the difference between the pairs in the same block using (2) with notations p_0, p_1, p_2, and p_3 for the first, second, and third differences, respectively.

$$\begin{cases} h_0 = p_0 - p_1 \\ h_1 = p_1 - p_1 \\ h_2 = p_2 - p_1 \\ h_3 = p_3 - p_1 \end{cases} \tag{2}$$

The obtained differences are arranged into two categories: ones that can be expanded, called expandable differences, and those that cannot be called non-expandable. The secret bits of data s are concealed in the expendable differences notated as h and expanded to $2h$, and the difference with private data becomes h' (see (3)). To find the pixel new pixel p' after data embedding, they use (4) to calculate adding h' to the original pixel of the cover image.

$$h' = 2h + S \tag{3}$$

$$P' = h' + p \tag{4}$$

For data extraction, the pixels of the stego image are arranged in quads, and by using the least significant bit (LSB) as of (5), the secret data s, is obtained.

$$S = LSB(h') \tag{5}$$

Their work shows promising results but needs to improve the PSNR and the payload capacity. Hence based on their work, we proposed a new scheme that operates on pairs of pixels with overlaps.

The research in [13] proposed another steganographic scheme to expand the differences in pixels arranged in pairs with a threshold value of the difference to decide on the pixel's embeddability. The methodology of their work is based on preprocessing the cover image with fuzzy logic and using DE to hide the secret bits. The preprocessing stage consists of first identifying the edges using fuzzy logic, followed by computing a key that maintains the relationship between the cover and its edges. Secondly, the random bits of the secret data before being embedded in the contents of the cover edge are multiplied by the key calculated during the preprocessing operation. After data embedding, they construct the stego image by multiplying the obtained values by the key calculated during data cover preprocessing. Their experimental results outperformed the ones obtained in [12]; however, the method was much more complex in the computational view though the results were promising in numbers. Therefore, we are proposing a new scheme to work on the original cover image, which is expected to be better than this in terms of computing complexity and yielding better results.

The research in [14] proposed a method for improved data hiding that utilizes difference expansion and modulus function on pixels grouped into blocks of pairs. The goal of this spatial-domain technique was to enhance payload capacity while maintaining a reasonable quality for the resulting stego image. The method proposed in their research involves hiding data in negative and positive differences between neighbouring pixels, using two ranges of values (-2 to 0 and 0 to 2) for data embedding. They apply a modulus two operation after pixel differences computation in the stego image to extract the confidential data. Their work's limitations are that it cannot be applied to large payloads because it considers a short range of differences that impacted the payload capacity, as many pixels were not used in embedding data.

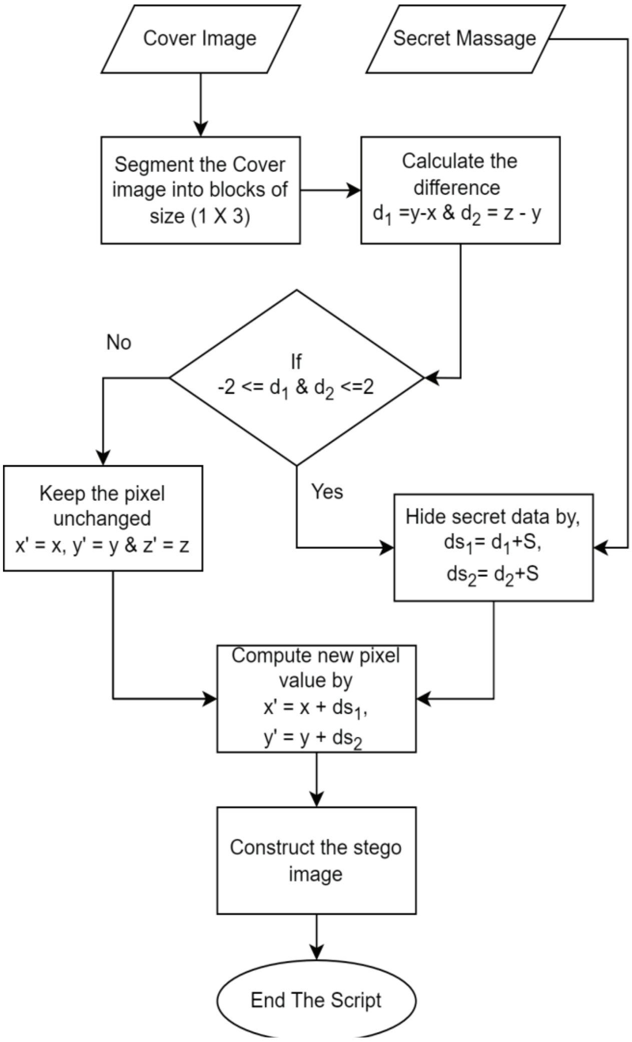

Cover Image
Secret Massage
Segment the Cover image into blocks of size (1 X 3)
Calculate the difference d1 =y-x & d2 = z - y
No
If -2 <= d1 & d2 <=2
Yes
Keep the pixel unchanged x' = x, y' = y & z' = z
Hide secret data by, ds1= d1+S, ds2= d2+S
Compute new pixel value by x' = x + ds1, y' = y + ds2
Construct the stego image
End The Script

Fig. 1 Embedding method

The study in [15] presents a method to improve the PSNR (BPP) based on the differencing pixel values. The method in their article combines pixel value ordering and the DE. Their approach consists of first sorting all the pixels of the cover in order, followed by pixels grouping in pairs based on their neighbourhoods. Next, the DE method without overlaps is applied to find the pixels with eligibility to be used in data embedding and, upon pixel eligibility confirmation, the data in the second position of the pairs. However, the results showed that a slight addition of the payload weakened the PSNR. Therefore, this work suggests the need for further improvement in the performance by considering overlapped differences in calculations.

III. Proposed Method

This work focuses on hiding secret data in the expanded differences. The differences are calculated with overlaps in the pixels arranged in blocks of triplets. Including the overlaps in the data-hiding process makes our approach unique compared to the existing works. Figure 1 illustrates a flowchart of the proposed approach, further explained in subsection A of this section. Nevertheless, hiding data should not be enough for the validity of a steganographic approach; therefore, Fig. 2 in subsection B summarizes the data extraction steps detailed in this subsection.

A. Data embedding process

In the embedding, our algorithm consists of three main stages: input, data concealment, and stego image generation. The algorithm in Fig. 1 is detailed in the following stages:

1) Stage 1: Arrange the pixels into blocks of three pixels with labels x for the first pixel at $row\ 1\ column\ 1$ notated as position (1,1), y for the second pixel at $row\ 1\ column\ 2$ notated as position (1,2), and z for the third pixel at $row\ 1\ column\ 3$ notated as position (1,3).

2) Stage 2: Compute the differences d_1 as the first difference and d_2 as a second difference obtained by involving y a second time that reflects the overlapping operation as (6).

$$\begin{cases} \mathrm{d}_1 = \mathrm{y} - \mathrm{x} \\ d_2 = \mathrm{z} - \mathrm{y} \end{cases} \quad (6)$$

3) Stage 3: Iterate through the differences to identify the ones that satisfy the condition: $-2 \leq d_1 \leq +2$ or $-2 \leq d_2 \leq +2$.

4) Stage 4: Hide the secret data in the selected differences that satisfy the condition in stage 3. To hide the data S, the differences d_1 or d_2 that complies with the condition will be added to the secret bits as of (7) and (8) to become the new differences ds_1 and ds_2

$$ds_1 = d_1 + S, \quad (7)$$

$$ds_2 = d_2 + S \quad (8)$$

5) Stage 5: Computing the pixels of the stego image x', y', and z' using (9) and (10).

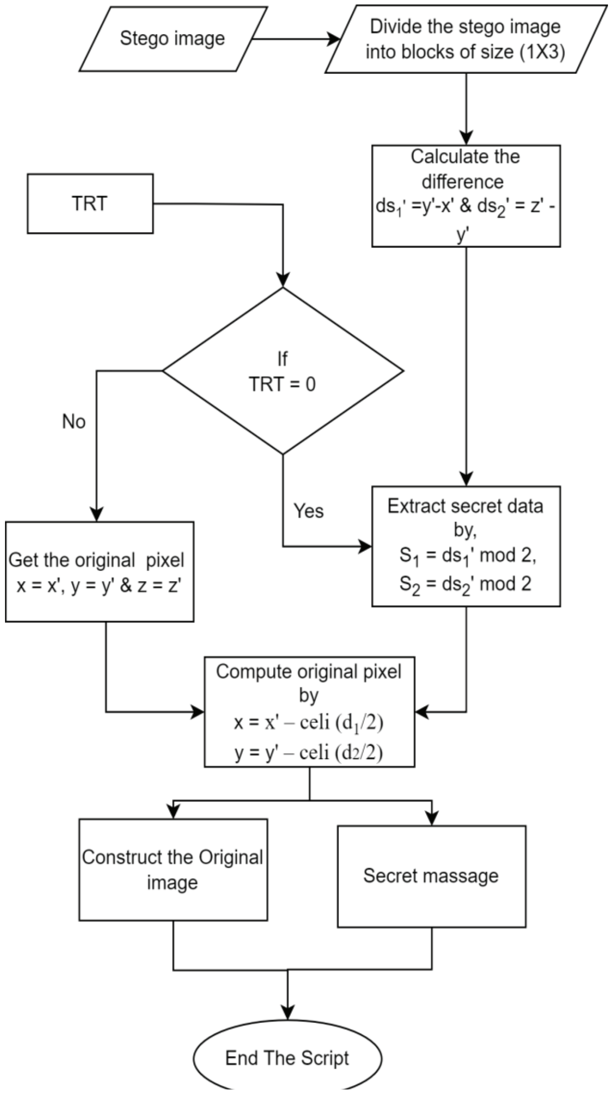
$$x' = x + (ds_1\ or\ ds_2) \quad (9)$$

$$y' = y + (ds_1\ or\ ds_2) \quad (10)$$

B. Data extraction process

For extracting confidential data from the stego image, we input a stego image and then work as per our algorithm in Fig. 2 as per the following stages:

1) Stage 1: Arranging the pixels of the stego image into triplets of size 1×3 and label them as x' for the first pixel at $row\ 1\ column\ 1$ notated as position (1,1), y' for the second pixel at $row\ 1\ column\ 2$ notated as position (1,2), and z' for the third pixel at $row\ 1\ column\ 3$ notated as position (1,3).



Stego image
Divide the stego image into blocks of size (1X3)
Calculate the difference $ds_1' = y' - x'$ & $ds_2' = z' - y'$
TRT
If TRT = 0
No
Yes
Extract secret data by, $S_1 = ds_1'$ mod 2, $S_2 = ds_2'$ mod 2
Get the original pixel x = x', y = y' & z = z'
Compute original pixel by x = x' – celi (d_1/2) y = y' – celi (d2/2)
Construct the Original image
Secret massage
End The Script

Fig. 2 Extraction method

2) Stage 2: Compute the differences labelled as ds_1' and ds_2' between the pixels x', y', and z' using (11) and (12).

$$ds_1' = y' - x' \quad (11)$$

$$ds_2' = z' - y' \quad (12)$$

3) Stage 3: Check the TRT table to see whether it is encrypted or not encrypted.$TRT = 0$ is encrypted and $TRT = 1$ is not encrypted pixel.

4) Stage 4: If TRT = 0, then, Extract the secret data $S_1\ and\ S_2$ modulus two operations on the differences from the previous stage as of (11) and (12). Furthermore, follow the equation (13) and (14).

$$S_1 = ds_1\ mod\ 2 \quad (13)$$

$$S_2 = ds_2\ mod\ 2 \quad (14)$$

After getting the secret data needed to construct the original cover image, to construct an original image, we calculate the original pixel by the equations (15) and (16).

$$x = x' - celi\left(\frac{y' - x'}{2}\right) \quad (15)$$

$$y = y' - celi\left(\frac{z'-y'}{2}\right) \quad (16)$$

If TRT = 1, there is no hidden data in that pixel.

So, the original image has not been altered by confidential data. Therefore, the pixels of the cover are got by (17):

$$\begin{cases} x = x' \\ y = y' \\ z = z' \end{cases} \quad (17)$$

IV. Experimental Results and Discussion

This section presents the experiment and the obtained results and is organized into two subsections. Subsection A describes the experimental setup, and subsection B presents and discusses the obtained results.

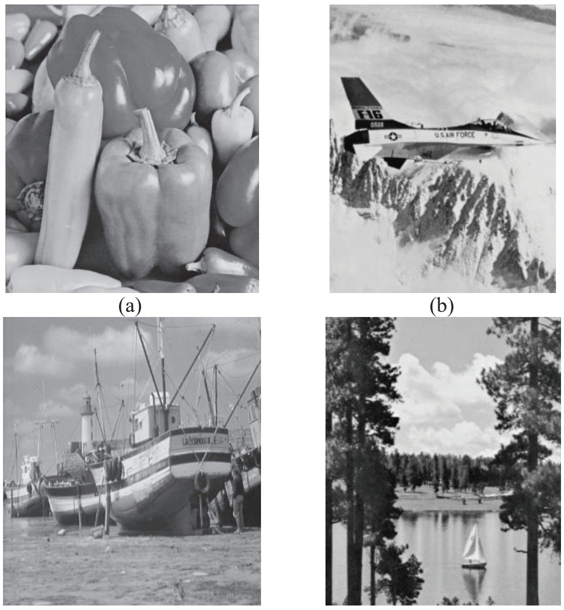
A. Experimental Setup

For the experiment, we use different cover images taken from SIPI Image Database [16], and for steganographic payloads, we use data bitstreams randomly generated with sizes $1kb$, $10kb$, $20kb$, $30kb$, $40kb$, $50kb$ and $100kb$. The images used are initially camera-taken images in the grayscale format and of size 512×512. Figure 3 shows sample images used as cover in our experiment. We use this dataset because of a comparison with the previous work. In the previous work dataset used by some authors, we used the same dataset as the cover image and hidden secret data.

Our method's evaluation metric is the PSNR computed using (18). The PSNR is dependent on the value of the mean square error (MSE) obtained by summating the squares of the differences between the pixels of the cover image $C(i,j)$ and the pixels of the stego image $S(i',j')$ As of (19), we are using this equation to reconstruct the original image. As we know, for reconstructing, we need to measure the quality of the image.

$$PSNR = 10.log_{10}\left(\frac{255^2}{MSE}\right) \quad (18)$$

$$MSE = \frac{1}{G\times H}\sum_{i=1}^{G}\sum_{j=1}^{H}[C1(i,j) - STI\ (i',j')]^2 \quad (19)$$


(a) (b) (c) (d)

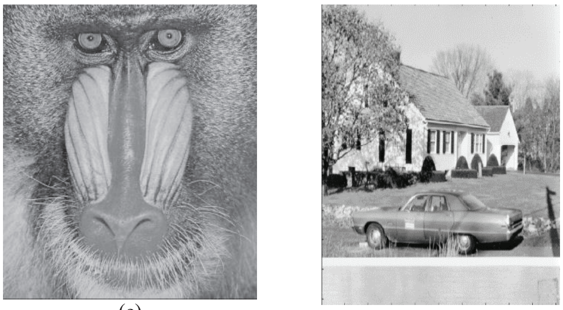

(e) (f)

Fig. 3 Sample images used in the experiment (a) Pepper (b) Airplane (c) Boat (d) Tree (e) Baboon (f) House

B. Results

Our results are compared to the existing work [14], as Fig. 4 shows a comparative portrait of the payload capacity yielded. Based on the graphs the in this figure, the proposed method is proved to outperform the existing method in the payload capacity when the PSNR is closely the same.

In addition, a comparative view of the PSNR is depicted in Fig. 5, using an exact size steganographic payload. It also shows the superiority of the proposed method over the existing method with a significant difference.

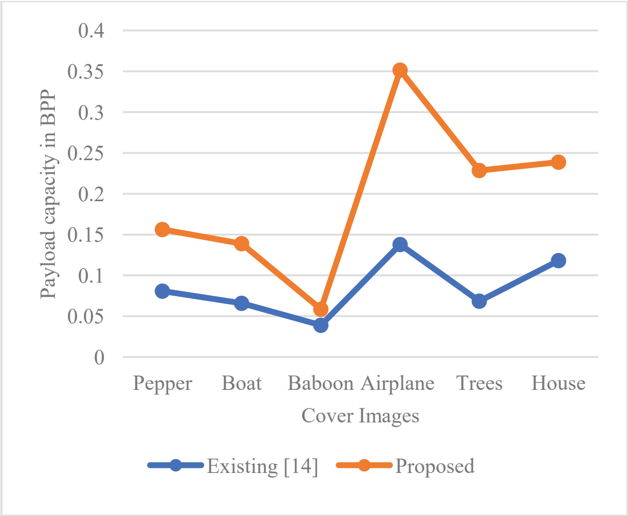


Fig. 4 Payload capacity result compared with the existing and proposed system.

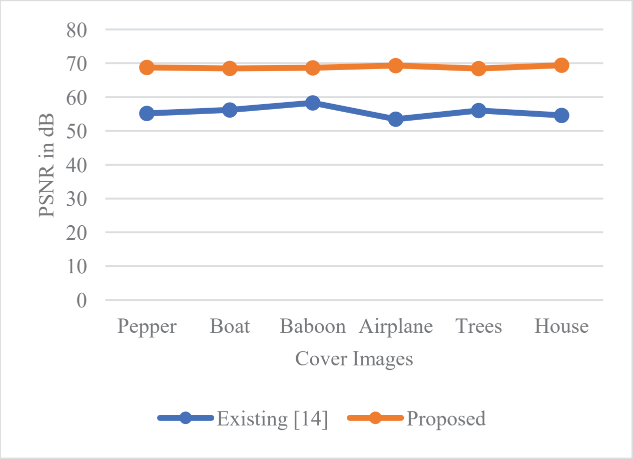


Fig. 5 PSNR result with the existing and proposed system.

TABLE I. PSNR AND PAYLOAD CAPACITY IN DIFFERENT SIZES OF PAYLOAD

Image	**The payload in (kb)**	**Proposed System**	
		PSNR in (dB)	**Payload Capacity (bpp)**
Pepper	1	68.7790	0.1562
	10	58.4500	
	20	55.4614	
	30	53.6887	
	40	52.4525	
	50	51.4942	
	100	50.8692	
Boat	1	68.4888	0.1389
	10	58.5146	
	20	55.4355	
	30	53.7046	
	40	52.4532	
	50	51.5326	
	100	51.3646	
Baboon	1	68.6613	0.0585
	10	58.2843	
	20	55.3368	
	30	54.4024	
	40	54.3933	
	50	54.4093	
	100	54.3863	
Airplane	1	69.3146	0.3514
	10	59.9170	
	20	56.2057	
	30	54.3493	
	40	53.0064	
	50	51.9451	
	100	49.3741	
Trees	1	68.4423	0.2285
	10	58.4973	
	20	55.6718	
	30	54.1643	
	40	53.0135	
	50	52.1435	
	100	50.3391	
House	1	69.4337	0.2387
	10	58.8439	
	20	56.1579	
	30	54.5680	
	40	53.3344	
	50	52.4423	
	100	50.8836	

Furthermore, we present the obtained results with the proposed method in Table I, which consists of the different values yielded in the PSNR and the payload capacity with various sizes of payloads.

V. CONCLUSION

This work presents a new steganographic approach that yields outperforming results over the existing works in terms of PSNR with increased payload capacity. Hence, the effect of the tradeoff between the payload capacity and the visibility quality of the stego image is reduced. In our method, we use the image's pixels grouping into blocks of triplets and then calculate the differences between the pixels of the identical triplet with overlaps. The consideration of overlap in differences calculations generate many embeddable areas compared to the methods with the previously proposed methods that do not consider overlaps. The experimentation of our algorithm is done with general-purpose grayscale images with random bitstreams as confidential data.

In the future, we aim to implement our algorithm with other techniques to preprocess the cover as of [13], for instance, to improve the stego image quality for high payload steganography.

REFERENCES

[1] Md. A. Islam, T. Tabassum, Md. S. Hossen, S. Hossain, M. Hossain, and A. H. Jony, "A Digital Data Hiding Technique with Missing Puzzle and Seek Algorithm," in *2020 4th International Conference on Electronics, Communication, and Aerospace Technology (ICECA)*, 2020, pp. 1304–1309. doi: 10.1109/ICECA49313.2020.9297600.

[2] I. B. Prayogi, T. Ahmad, N. J. de La Croix, and P. Maniriho, "Hiding Messages in Audio using Modulus Operation and Simple Partition," in *Proceedings of 2021 13th International Conference on Information and Communication Technology and System, ICTS 2021*, 2021, pp. 51–55. DOI: 10.1109/ICTS52701.2021.9609028.

[3] J. Chang, F. Ding, X. Li, and G. Zhu, "Hybrid prediction-based pixel-value-ordering method for reversible data hiding," *J Vis Commun Image Represent*, vol. 77, May 2021, DOI: 10.1016/J.JVCIR.2021.103097.

[4] Y. Wang, G. Xiong, and W. He, "High-capacity reversible data hiding in encrypted images based on pixel-value-ordering and histogram shifting," *Expert Syst Appl*, vol. 211, p. 118600, Jan. 2023, DOI: 10.1016/J.ESWA.2022.118600.

[5] W. Ding, H. Zhang, R. Reulke, and Y. Wang, "Reversible image data hiding based on scalable difference expansion," *Pattern Recognit Lett*, vol. 159, pp. 116–124, Jul. 2022, DOI: 10.1016/j.patrec.2022.05.014.

[6] J. Chang, F. Ding, X. Li, and G. Zhu, "Hybrid prediction-based pixel-value-ordering method for reversible data hiding," *J Vis Commun Image Represent*, vol. 77, May 2021, DOI: 10.1016/j.jvcir.2021.103097.

[7] H. Wu, X. Li, Y. Zhao, and R. Ni, "Improved PPVO-based high-fidelity reversible data hiding," *Signal Processing*, vol. 167, Feb. 2020, DOI: 10.1016/j.sigpro.2019.107264.

[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] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, DOI: 10.1016/j.neucom.2018.06.075.

[10] M. Hussain, A. W. A. Wahab, Y. I. bin Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Process Image Commun*, vol. 65, pp. 46–66, Jul. 2018, DOI: 10.1016/j.image.2018.03.012.

[11] G. Kaur, S. Singh, and R. Rani, "A High Capacity Reversible Data Hiding Technique Based on Pixel Value Ordering Using Interlock Partitioning," in *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2020, pp. 727–732. DOI: 10.1109/SPIN48934.2020.9071330.

[12] M. Ntahobari and T. Ahmad, "Protecting data by improving quality of stego image based on enhanced reduced difference expansion," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 4, pp. 2468–2476, Aug. 2018, DOI: 10.11591/ijece.v8i4.pp2468-2476.

[13] N. J. de La Croix, C. C. Islamy, and T. Ahmad, "Secret Message Protection using Fuzzy Logic and Difference Expansion in Digital Images," in *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022*, 2022. DOI: 10.1109/NIGERCON54645.2022.9803151.

[14] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of King Saud University - Computer and Information*

Sciences, vol. 31, no. 3, pp. 335–347, Jul. 2019, DOI: 10.1016/j.jksuci.2018.01.011.

[15] 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)*, Nov. 2022, pp. 33–38. DOI: 10.1109/COMNETSAT56033.2022.9994516.

[16] "SIPI Image Database - Misc." https://sipi.usc.edu/database/database.php?volume=misc (accessed Dec. 10, 2022).