Reversible difference expansion multi-layer data hiding technique for medical images

Pascal Maniriho [a,1], Leki Jovial Mahoro [b,2], Zephanie Bizimana [a,3], Ephrem Niyigaba [a,4], Tohari Ahmad [c,5,*]

[a] Department of Information and Communication Technology, Rwanda Polytechnic-IPRC Karongi, Karongi 85, Rwanda
[b] Department of Information Technology, Vaal University of Technology, Vanderbijlpark 19000, South Africa
[c] Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), Surabaya, 60111, Indonesia
[1] pmaniriho@iprckarongi.rp.ac.rw; [2] lekim@vut.ac.za; [3] bizimana@iprckarongi.rp.ac.rw; [4] ictdepartment@iprckarongi.rp.ac.rw;
[5] tohari@if.its.ac.id
* corresponding author

ARTICLE INFO

Article history
Received April 7, 2020
Revised November 15, 2020
Accepted December 17, 2020
Available online March 31, 2021

Keywords
Data hiding
Data protection
Data security
Digital content
Information security

ABSTRACT

Maintaining the privacy and security of confidential information in data communication has always been a major concern. It is because the advancement of information technology is likely to be followed by an increase in cybercrime, such as illegal access to sensitive data. Several techniques were proposed to overcome that issue, for example, by hiding data in digital images. Reversible data hiding is an excellent approach for concealing private data due to its ability to be applied in various fields. However, it yields a limited payload and the quality of the image holding data (Stego image), and consequently, these two factors may not be addressed simultaneously. This paper addresses this problem by introducing a new non-complexity difference expansion (DE) and block-based reversible multi-layer data hiding technique constructed by exploring DE. Sensitive data are embedded into the difference values calculated between the original pixels in each block with relatively low complexity. To improve the payload capacity, confidential data are embedded in multiple layers of grayscale medical images while preserving their quality. The experiment results prove that the proposed technique has increased the payload with an average of 369999 bits and kept the peak signal to noise ratio (PSNR) to the average of 36.506 dB using medical images' adequate security the embedded private data. This proposed method has improved the performance, especially the secret size, without reducing much the quality. Therefore, it is suitable to use for relatively big payloads.

1. Introduction

Data hiding approaches can be employed to solve many security issues recently encountered in the transmission and sharing of multimedia digital content (confidential data such as audio, text, video, and image). In data hiding, data security is achieved by embedding the secret data into the host media, which is performed by substituting the insignificant or redundant digits of the host for the ones from the confidential information. The goal is to allow data to be shared through unknown (hidden) communication, which keeps data transmission only between the source and the intended destination. Recently, different data hiding techniques have been implemented to protect digital content from being accessed illegally.

Reversible data hiding (R-DH) is one of the most popular approaches for authenticating and protecting data in many fields, such as medical imagery and military (defense), due to its ability to reproduce the host image and hidden payload after the extraction process. In this R-DH image-based technique, confidential data are concealed by modifying some parts (pixels) of the host image, which introduces distortion in the image and can, in turn, lead to security breakage or suspicion of the hidden data. If the capacity of payload held by the host image is high, its quality degrades. Since the recipient has to recover both the concealed payload and the original host, the image holding data's quality must be preserved. Conventional (irreversible) data hiding is another technique that only recovers the hidden payload and leaves the host media unrestored. In both cases, the payload capacity and Stego image's quality should always be achieved [1].

Nevertheless, previous research has revealed that there is always a trade-off between the capacity and the quality encountered in data hiding approaches. Thus, maintaining variation of these factors is among the major concerns. In other words, caution should be taken to maintain an adequate balance between them [2][3]. Several approaches have been implemented to enhance one or both factors. For instance, to decrease the distortion level, secret data were concealed into the reduced difference values [4]. Efficient embedding capacity was implemented by exploiting the parity-bit differencing in the scheme developed by Hussain et al. [5]. Some approaches are also implemented in the frequency domain where data hiding is performed by first transforming the host image using certain algorithms such as Fast Fourier Transform and Wavelet Transform. An example of such an approach was presented in Hu *et al.* [6].

Additionally, another technique based on histogram shifting and difference selection schemes was further presented to enhance the existing schemes. Their results demonstrate that the capacity was improved up to 0.5 bpp. A new method was implemented by combining modulus function and difference expansion (DE), which significantly achieves a high embedding capacity, and PSNR was proposed in [7]. Other reversible methods were presented in [8][9]. Forward and backward direction mechanisms coupled with a different pair mapping scheme were developed in [10].

Furthermore, a prediction based on an arbitrary threshold method was applied to exploit the cover media's statistical characteristic to enhance the size of the payload. The goal of the predicted values is to provide security of information to conceal. The Stego media quality was enhanced in a lossless scheme that considers similarities between adjacent pixels in each block of pixel [11]. Yadav and Ojha [12] have used the Hilbert curve and logistic map to implement a new R-DH method with enhanced embedding capacity. Other R-DH approaches were presented in [13]-[18]. This paper presents a new non-complexity DE and block-based reversible multi-layer data hiding technique that intends to enhance the capacity of payload and preserve the Stego media's quality without any complexity as data are easily concealed in the difference computed between pixels in each block. Unlike the previous approaches that conceal data in one layer of the host media, which may result in a low payload capacity, our approach conceals data in more than one layer of medical grayscale images, which essentially enhance the payload.

The rest of this work is presented as follows. A brief overview of the functionality of R-DH based on DE techniques is presented in Section 2, which is followed by the proposed technique (data concealment and extraction phases). Section 3 provides a detailed discussion of the results of the experiment. The conclusion of this work is given in Section 4.

2. Method

In this section, we explain the method, preceded by its underlying approach. Variations of this basic scheme are also provided.

2.1. Difference Expansion

Many different expansion–based data hiding approaches have been presented in the previous work [19] [20]. The DE is a data embedding approach that protects data by hiding them into different values. DE-based schemes have become famous in the last two decades due to their reversibility characteristics, allowing the host image and protected confidential data to be reconstructed without deformation. Tian's method [21] is one of the existing DE-based schemes that has achieved a high embedding and acceptable quality of image holding the embedded data. Some variants of Tian's approaches have been developed such as those in [12], [19], and [22]-[30]. Overall, all of these techniques are employed to maintain users' security and privacy [21] and to minimize human errors in cybersecurity [21]. A typical image-based R-DH process is provided in Fig. 1, and basic steps explaining Tian's approach's functionality are discussed below. In the beginning, non-overlapped pixels are taken in pairs; thereafter, the mean (Y) and difference (h) are computed for each pair of pixels using (1) and (2), respectively. Note that Tian's algorithm [21] is reversible, and (j, g) represents pixels' pairs of the host media before embedding data.

$$Y = \left\lfloor \frac{j+g}{2} \right\rfloor \quad (1)$$

$$h = |\, j - g| \quad (2)$$

Tian's technique [21] conceals data (s) by expanding the difference (h) as shown in (3).

$$h' = 2 \times h + s \quad (3)$$

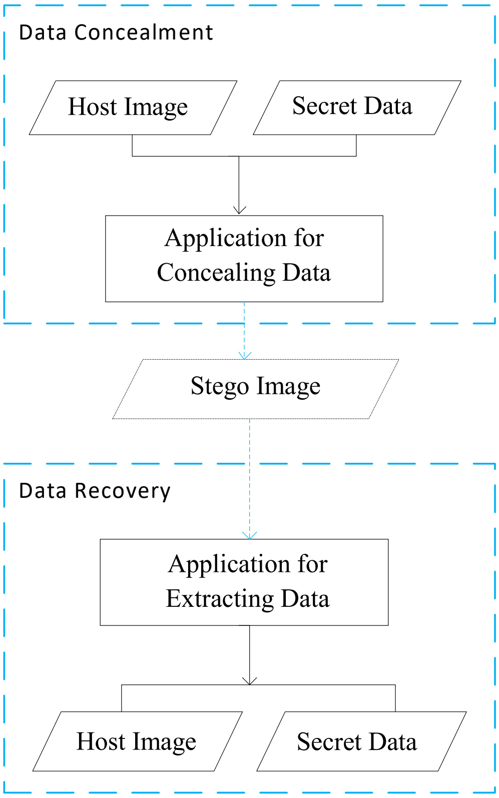


Fig. 1. A typical reversible Image-based data hiding technique

The expanded pair of pixels(j', g'), which are used to construct the Stego image, was calculated using the expressions in (4) and (5). Moreover, h' must fulfill (6) and (7) in order to avoid underflow and overflow problems.

$$j' = y + \left\lfloor \frac{h'+1}{2} \right\rfloor \quad (4)$$

$$g' = y - \left\lfloor \frac{h'}{2} \right\rfloor \quad (5)$$

$$|h'| \leq 2 \times (255 - y) \quad \text{if } 128 \leq y \leq 255 \quad (6)$$

$$|h'| \leq 2 \times y + 1 \quad \text{if } 128 \leq y \leq 127 \quad (7)$$

The difference (h") from each pair of pixels(j' , g'), which is obtained in (8) was used to recover the secret data (s) by $s = h'' mod\ 2$. After that, the original difference and the original pair of pixels (j, g) were restored by applying (9) and (10), where y' is the mean of (j' , g') and h is the original difference obtained after right shifting (h") → $h = floor\ h''$. Note that with Tian's approach, both the embedded payload and host media were restored.

$$h'' = |\, j' - g' | \tag{8}$$

$$j = y' + \left\lfloor \frac{h+1}{2} \right\rfloor \tag{9}$$

$$g = y' - \left\lfloor \frac{h}{2} \right\rfloor \tag{10}$$

2.2. Multi-Layer R-DH Technique

The proposed method that aims at hiding data in multiple layers of medical images is elaborated in this section. It is motivated by Tian's DE-based scheme [21] and the data embedding technique proposed in [11]. More specifically, we propose a new non-complexity DE and block-based reversible multi-layer data hiding technique that intends to increase the payload capacity while preserving the Stego media's quality. With this technique, the hiding process is first performed. The Stego image generated after the embedding of data can be transmitted over the network, and the authorized recipient will only extract the hidden data during the extraction process.

2.2.1. Secret Data Concealment Phase

Given an original host medical image, the entire process for embedding confidential data is elaborated as follows.

- Split the cover image into non-overlapped pixels' block of the same size (dimension) given by $n \times n$ where n can be an integer number, $\forall\, n\ \in\ Z$.
- Determine the position (p) of the base pixel (b_p) in each block of pixels by applying (11).

$$Position\ (p) = n \times n \tag{11}$$

As computed in (11), the position (p) of the base pixel in each block is determined by the dimension of the respective block. For example, if the dimension of a pixel block is represented by (n by) → ($n \times n$), where $n = 2$, which gives 2 × 2, then the position (p) is given by 4. This implies that the pixel at the fourth position can be taken as b_p.

- Utilize the b_p to compute the difference (w) → (12) where j represents the original pixel.

$$w = j - b_p \tag{12}$$

- Expand (w) to conceal the secret data (s) in multiple layers of the host image using (13), where the number of layers is given by (14). The variable holding the layers for embedding is increased until the PSNR value reaches 30 dB, and after that number of layers can no longer be incremented.

$$w' = 2 \times w + s \tag{13}$$

$$layer = layer + 1\ if\ PSNR\ > 30dB \tag{14}$$

- Compute the Stego pixel (j') by utilizing (15)

$$j' = b_p + w' \tag{15}$$

2.2.2. Extracting Embedded Data and Recovering the Cover Image

Extracting the hidden payload and recovering the cover media are performed by dividing the Stego media into non-overlapped blocks with the size $(n \times n)$; thereafter, the base pixel is computed in each block by applying the expression in (11). The base pixel is then used to compute the difference (w'') as shown in (16), while (17) is applied to recover secret data and (18) restores the host image.

$$w'' = j' - b_p \tag{16}$$

$$s = w'' - 2 \times \left\lfloor \frac{w''}{2} \right\rfloor \tag{17}$$

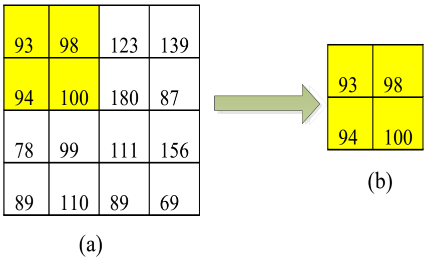
$$j = b_p - \left\lfloor \frac{w''}{2} \right\rfloor \tag{18}$$

The example illustrating the application of the proposed method is elaborated below. Given a block of pixels of size 2 by 2 → (2×2) represented in Fig. 2, which is generated from the host medical image (M) and the data secret (s)→ (101) to be embedded, the embedding process can be accomplished. Considering the criterion in (12), the base pixel for the given block is 100. Then, we compute the difference (w) between all pixels using the base pixel provided in (19), (20) and (21).

$$w_1 = |93 - 100| = 7 \tag{19}$$

$$w_2 = |98 - 100| = 2 \tag{20}$$

$$w_3 = |94 - 100| = 6 \tag{21}$$



93	98	123	139
94	100	180	87
78	99	111	156
89	110	89	69

(a)

93	98
94	100

(b)

Fig. 2. (a) Original host image M (b) Block of pixels

Having the difference values, secret bits can be concealed, as shown in (22), (23), and (24). Note that the base pixel is kept unchanged while Fig. 3 shows the embedding process where the cover image (host image) is first divided into pixels' block of the same size, and thereafter, the difference is computed between pixels. The data are concealed on multi-layers of the image and the process terminates once the PSNR reaches 30 dB. Besides, in order to ensure that all Stego pixels fall in the range $(0 \leq pixel\ value \leq 255)$, the lookup table is used to distinguish pixels that are changed and those which are not altered. More specifically, bits 1 in the lookup table indicates that the pixel value is changed while 0 is assigned to unchanged pixels.

$$w'_1 = (2 \times 7) + 1 = 15 \tag{22}$$

$$w'_2 = (2 \times 2) + 0 = 4 \tag{23}$$

$$w'_3 = (2 \times 6) + 1 = 13 \tag{24}$$

Obtain Stego pixels using the expanded difference values $(w'_1,\ w'_2,\ w'_3)$ and the base pixel by using (25), (26) and (27).

$$j' = 100 + 15 = 115 \tag{25}$$

$$j' = 100 + 4 = 104 \tag{26}$$

$$j' = 100 + 13 = 113 \tag{27}$$

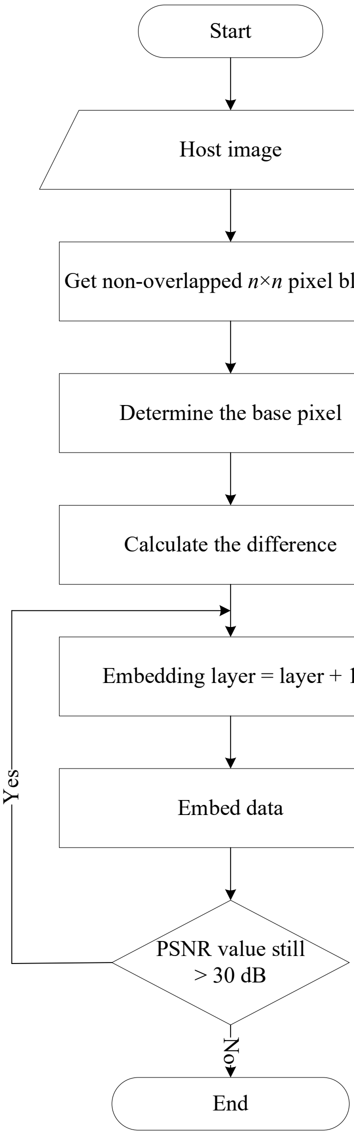


Fig. 3. Steps illustrating the embedding of the secret data

The pixels for constructing the Stego image are becoming 115, 104, 113 and b_p is 100, which is not altered. Let us now perform the recovery process. As it was discussed earlier, the difference is computed in (28), (29) and (30), the hidden secret data are first extracted as performed in (31), (32), and (33).

$$w_1 = |115 - 100| = 15 \tag{28}$$

$$w_2 = |104 - 100| = 4 \tag{29}$$

$$w_3 = |113 - 100| = 13 \tag{30}$$

$$s = 15 - 2 \times \left\lfloor \frac{15}{2} \right\rfloor = 1 \tag{31}$$

$$s = 4 - 2 \times \left\lfloor \frac{4}{2} \right\rfloor = 0 \tag{32}$$

$$s = 13 - 2 \times \left\lfloor \frac{13}{2} \right\rfloor = 1 \tag{33}$$

While the pixels (j) of the host image can also be recovered by applying expression in (18) as computed in (34), (35), and (36).

$$j = 100 - \left\lfloor \frac{115-100}{2} \right\rfloor = 93 \tag{34}$$

$$j = 100 - \left\lfloor \frac{104-100}{2} \right\rfloor = 98 \tag{35}$$

$$j = 100 - \left\lfloor \frac{113-100}{2} \right\rfloor = 94 \tag{36}$$

Considering the extracted secret data and the original pixels, it could be concluded that there is no mismatch in data, i.e., the process is trustworthy. Fig. 4 depicts the extraction procedures that are controlled by the number of layers (k), which were used in the embedding process. The data are extracted in each layer, and the process ends once the number of layers is less than one.

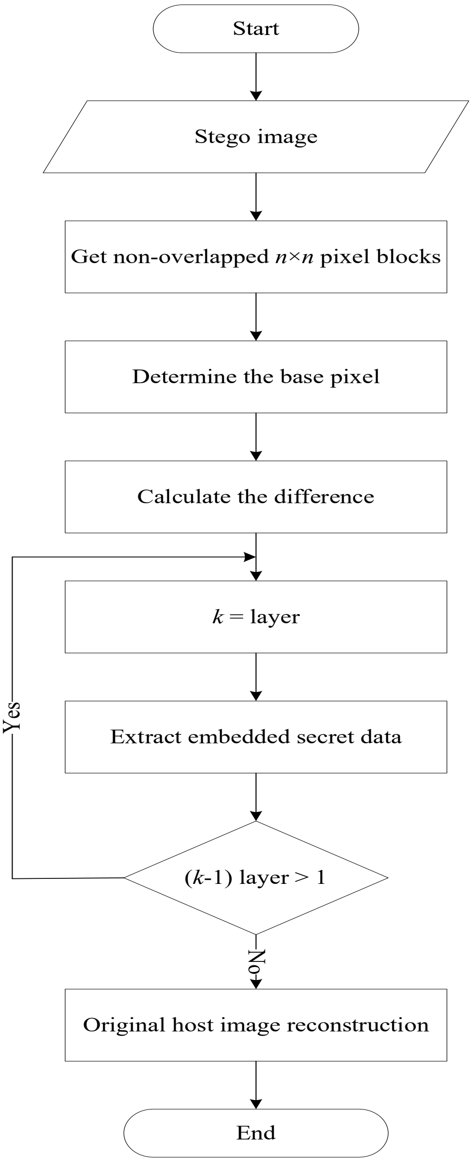

Start
Stego image
Get non-overlapped $n \times n$ pixel blocks
Determine the base pixel
Calculate the difference
k = layer
Extract embedded secret data
(k-1) layer > 1
Yes
No
Original host image reconstruction
End

Fig. 4. Steps illustrating the extraction of the hidden secret data.

3. Results and Discussion

The experimental analysis for the proposed non-complexity multi-layer DE method is presented in this section. The experiment is conducted using grayscale medical images of size 512 × 512 (presented in Fig. 5), which are taken from [31]. The payload capacity and PSNR are evaluated throughout the experiment. The PSNR is calculated as in [32], and it is employed to evaluate how the host image is degraded after concealing data. It does assess how the host image gets distorted in relation to the embedded secret data's capacity.

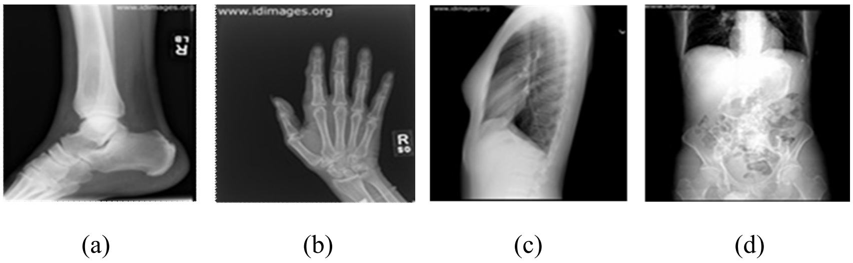

(a) (b) (c) (d)

Fig. 5. Tested grayscale host medical images: (a) Leg (b) Hand (c) Lung (d) Abdominal [31].

Table 1 presents the results (payload capacity in bits and PSNR in decibels (dB)) obtained after embedding the secret data in 3 layers of Leg, Hand, and Abdominal original medical images. Referring to the results, it could be seen that increasing the number of the embedding layers decreases the quality of the host media (which is computed in terms of PNSR). However, as depicted in Fig. 3, there is a criterion that controls the embedding so as to prevent the host image from being greatly changed, which can lead to data privacy and security issues. That is, to maintain a satisfactory payload capacity and Stego media's quality, the number of layers is increased whenever the PSNR is still higher than thirty decibels (PSNR > 30 dB). Once the threshold (30 dB) has been achieved, no further increment can be made.

Table 1. Embedding capacity and PSNR for Leg, Hand, and Abdominal Host image using the Proposed Method

Host Image	No. Layer	Capacity (Bits)	PSNR (dB)
Leg	1	124509	42.732
	2	124506	37.380
	3	124338	32.634
Hand	1	128250	41.776
	2	128250	36.3962
	3	127941	32.323
Abdominal	1	108540	41.299
	2	108540	35.673
	3	108438	31.333

Considering Leg original image after embedding confidential data in 3 layers, it could be seen that it does accommodate: layer 1 = 124509 bits, layer 2 = 124506 bits, and layer 3 = 124338 bits with the PSNR value of 42.732, 37.380, and 32.634. Additionally, it can also be seen that 373353 total number of embedded secret bits with the PSNR average of 37.582 dB is achieved after concealing the confidential data in 3 layers. It is worth noting that further embedding layers can be added, provided that the condition for embedding is fulfilled. Besides, all pixels of the host image are not used for concealing data, and the reason is that some pixel values do not fall within the grayscale range ($0 \leq pixel\ value \leq 255$) after embedding. Only those pixels which are within the range are considered for concealing the given private data. The comparison of the performance of the proposed method against one of the previous approaches is provided in Table 2, which reveals how the proposed method accommodates more bits than the previous method [33] for all host images.

Table 2. Results of the Proposed Approach and that in [33] by Considering Capacity and PSNR

Host Image	Capacity (Bits)		PSNR (dB)	
	The method in [33]	*Proposed Method*	*The Method in* [33]	*Proposed Method*
Leg	196605	373353	38.385	37.582
Hand	196587	384441	38.371	36.831
Abdominal	189408	325518	37.285	36.101
Lung	186948	396687	35.947	35.510

Fig. 6(a) and Fig. 6(b) are presented to show how the image's quality was preserved after concealing data in different layers of the host image. By considering both Fig 6(a) and Fig. 6(b), which are the Stego images after embedding data in the first and second layers, respectively, we could see that although the PSNR values are a bit different (with the PSNR difference value of 5.352 dB), both images are almost identical. It may assure that the privacy and security of the hidden data during data communication. This means that the Stego image cannot be easily suspected during data transmission over the network. This condition keeps the authenticity and confidentiality of the confidential data to be shared. The proposed multi-layer R-HD method could be applied in information security areas, where the security of data and privacy have to be maintained to avoid security breaches throughout confidential data sharing.

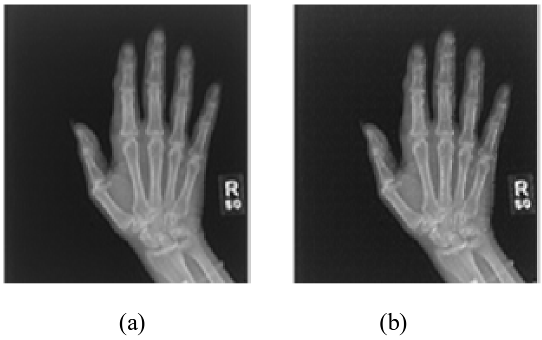


Fig. 6. Examples of Stego image after embedding secret data in Hand medical image (a) Layer 1, capacity = 128250 bits and PSNR = 42.732 dB (b) Layer 2, capacity = 124506 bits and PSNR = 37.380 dB

4. Conclusion

A new non-Complexity DE and block-based multi-layer R-DH technique that embeds confidential data into more than one layer of original medical cover images is presented in this work. The proposed method can hide a satisfactory payload and keep Stego's quality at a reasonable level. However, there is a decrease in the PSNR whenever the number of layers is increased. In order to ensure that there is no suspicion or data security breakage that can be raised against the Stego media, the proposed approach controls the increment of the embedding layers. As a result, confidential data can be concealed in medical grayscale images with less complexity and degradations with this approach. In turn, this process preserves the privacy and security of the embedded confidential information. Therefore, this approach can be employed to protect private data's confidentiality and integrity during transmission over the internet. Nevertheless, increasing the number of layers improves the payload capacity while decreasing the host media's quality. So, those two factors should be chosen appropriately. Inspite of its advantages, this proposed method has some limitations, as previously described. In the future, we would like to overcome them by applying a pixel value ordering approach to maintain the quality of the Stego media. Furthermore, the pixel blocks' size may be varied to find an appropriate number of pixels to use, besides the order and the composition of each block. Other possible types of cover may also be investigated. It is to find whether the approach also works well in different environments, considering that they have different characteristics. The performance may be affected.

Acknowledgment

We thank all members of Net-Centric Computing Laboratory who have supported this research.

Declarations

Author contribution. Pascal Maniriho: designing methodology, coding, experiment, writing; Leki Jovial Mahoro: designing methodology, analyzing; Zephanie Bizimana: designing methodology, reviewing; Ephrem Niyigaba: designing methodology, reviewing; and Tohari Ahmad: reviewing, editing, supervision, funding.

Funding statement. This research was supported by the Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia.

Conflict of interest. The authors declare no conflict of interest.

Additional information. No additional information is available for this paper.

References

[1] X. Zhang, "Reversible Data Hiding With Optimal Value Transfer," *IEEE Trans. Multimed.*, vol. 15, no. 2, pp. 316–325, 2013. doi: 10.1109/TMM.2012.2229262.

[2] B. Ou, X. Li, and W. Zhang, "PVO-Based Reversible Data Hiding For Encrypted Images," in *IEEE China Summit and International Conference on Signaland Information Processing*, 2015, pp. 831–835. doi: 10.1109/ChinaSIP.2015.7230521.

[3] W. Hong, T. Chen, and J. Chen, "Reversible data hiding using Delaunay triangulation and selective embedment," *Inf. Sci. (Ny).*, 2014, doi: 10.1016/j.ins.2014.03.030.

[4] P. Maniriho and T. Ahmad, "Enhancing the Capability of Data Hiding Method Based on Reduced Difference Expansion," *Eng. Lett.*, vol. 26, no. 1, pp. 45–55, 2018. Available at: Google Scholar.

[5] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, 2006. doi: 10.1109/LCOMM.2006.060863.

[6] Y. Hu, H. Lee, K. Chen, and J. Li, "Hiding Using Two Embedding Directions," vol. 10, no. 8, pp. 1500–1512, 2008. doi: 10.1109/TMM.2008.2007341.

[7] P. Maniriho and T. Ahmad, "Information Hiding Scheme for Digital Images Using Difference Expansion and Modulus Function," *J. King Saud Univ. - Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2018.01.011.

[8] Y. Kurniawan, L. A. Rahmania, T. Ahmad, W. Wibisono, and R. M. Ijtihadie, "Hiding Secret Data by using Modulo Function in Quad Difference Expansion," in *International Conference on Advanced Computer Science and Information Systems (ICACSIS 2016)*, 2016, pp. 433–437. doi: 10.1109/ICACSIS.2016.7872741.

[9] H. S. El-sayed, S. F. El-Zoghdy, and O. S. Faragallah, "Adaptive Difference Expansion-Based Reversible Data Hiding Scheme for Digital Images," *Arab. J. Sci. Eng.*, vol. 41, no. 3, pp. 1091–1107, 2016, doi: 10.1007/s13369-015-1956-7.

[10] V. K. C, V. Natarajan, and S. M. S, "Difference Expansion based Reversible Data Hiding for Medical Images," pp. 720–723, 2014, doi: 10.1109/ICCSP.2014.6949937.

[11] M. Khodaei and K. Faez, "Reversible Data Hiding By Using Modified Difference Expansion," in *2010 2nd International Conference on Signal Processing Systems (ICSPS)*, 2010, no. 5, pp. 31–34. doi: 10.1109/ICSPS.2010.5555649.

[12] G. S. Yadav and A. Ojha, "A Reversible Data Hiding Scheme with High Security and Improved Embedding Capacity," in *2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference on Big Data Science And Engineering*, 2018, pp. 1555–1559, doi: 10.1109/TrustCom/BigDataSE.2018.00223.

[13] A. Mohammadi, M. Nakhkash, and M. A. Akhaee, "A High-Capacity Reversible Data Hiding in Encrypted Images Employing Local Difference Predictor," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 8, pp. 2366–2376, 2020, doi: 10.1109/TCSVT.2020.2990952.

[14] J. He, J. Chen, and S. Tang, "Reversible Data Hiding in JPEG Images Based on Negative Influence Models," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. c, pp. 2121–2133, 2019, doi: 10.1109/TIFS.2019.2958758.

[15] X. Yin, W. Lu, W. Liu, J.-M. Guo, J. Huang, and Y.-Q. Shi, "Reversible Data Hiding in Halftone Images Based on Dynamic Embedding States Group," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8215, no. c, pp. 1–1, 2020, doi: 10.1109/TCSVT.2020.3032685.

[16] 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*, 2020, pp. 727–732, doi: 10.1109/SPIN48934.2020.9071330.

[17] F. Aziz, T. Ahmad, A. H. Malik, M. I. Uddin, S. Ahmad, and M. Sharaf, "Reversible data hiding techniques with high message embedding capacity in images," *PLoS One*, vol. 15, no. 5, 2020, doi: 10.1371/journal.pone.0231602.

[18] H. Wu, "Patch-Level Selection and Breadth-First Prediction Strategy for Reversible Data Hiding," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2020, pp. 2837–2841, doi: 10.1109/ICASSP40776.2020.9054386.

[19] W. Wang, J. Ye, T. Wang, and W. Wang, "Reversible data hiding scheme based on significant-bit-difference expansion," *IET Image Process.*, pp. 1002–1014, 2017, doi: 10.1049/iet-ipr.2017.0151.

[20] V. Kumar and V. Natarajan, "Hybrid local prediction error-based difference expansion reversible watermarking for medical images," *Comput. Electr. Eng.*, vol. 53, pp. 333–345, 2016, doi: 10.1016/j.compeleceng.2015.11.033.

[21] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, 2003, doi: 10.1109/TCSVT.2003.815962.

[22] D. Coltuc and A. Tudoroiu, "Multibit Versus Multilevel Embedding In High Capacity Difference Expansion Reversible Watermarking," in *20th European Signal Processing Conference (EUSIPCO 2012)*, 2012, pp. 1791–1795. Available at: Google Scholar.

[23] H. Yi, S. Wei, and H. Jianjun, "Improved Reduced Difference Expansion Based Reversible Data Hiding Scheme for Digital Images," in *9th International Conference on Electronic Measurement & Instruments, 2009. ICEMI '09.*, pp. 315–318. doi: 10.1109/ICEMI.2009.5274054.

[24] R. Kumar and K. H. Jung, "Robust reversible data hiding scheme based on two-layer embedding strategy," *Inf. Sci. (Ny).*, vol. 512, pp. 96–107, 2020, doi: 10.1016/j.ins.2019.09.062.

[25] R. Kumar, D. S. Kim, and K. H. Jung, "Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing," *J. Inf. Secur. Appl.*, vol. 47, pp. 94–103, 2019, doi: 10.1016/j.jisa.2019.04.007.

[26] H. Yao, F. Mao, Z. Tang, and C. Qin, "High-fidelity dual-image reversible data hiding via prediction-error shift," *Signal Processing*, vol. 170, p. 107447, 2020, doi: 10.1016/j.sigpro.2019.107447.

[27] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *J. King Saud Univ. - Comput. Inf. Sci.*, 2019, doi: 10.1016/j.jksuci.2019.07.004.

[28] P. Chowdhuri and B. Jana, "Hiding data in dual color images reversibly via weighted matrix," *J. Inf. Secur. Appl.*, vol. 50, 2020, doi: 10.1016/j.jisa.2019.102420.

[29] S. Bhalerao, I. A. Ansari, A. Kumar, and D. K. Jain, "A reversible and multipurpose ECG data hiding technique for telemedicine applications," *Pattern Recognit. Lett.*, vol. 125, pp. 463–473, 2019, doi: 10.1016/j.patrec.2019.06.004.

[30] D. Huang and J. Wang, "High-capacity reversible data hiding in encrypted image based on specific encryption process," *Signal Process. Image Commun.*, vol. 80, no. September 2019, p. 115632, 2020, doi: 10.1016/j.image.2019.115632.

[31] "Partners Infectious Disease Images - eMicrobes Digital Library - Home.". Available at: idimages.org.

[32] S. Chen, "A module-based LSB substitution method with lossless secret data compression," *Comput. Stand. Interfaces*, vol. 33, no. 4, pp. 367–371, 2011, doi: 10.1016/j.csi.2010.11.002.

[33] T. Ahmad, M. Holil, W. Wibisono, and I. Royyana Muslim, "An improved Quad and RDE-based medical data hiding method," in *International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM)*, 2013, pp. 141–145, doi: 10.1109/CyberneticsCom.2013.6865798.