International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 6
ISSN: 2088-5334

Data Hiding Scheme Based on Quad General Difference Expansion Cluster

Ahmad Juniar Ilham [a], Tohari Ahmad [b,*], Ntivuguruzwa Jean De La Croix [b,c], Pascal Maniriho [d], Maurice Ntahobari [e]

[a] *Department of Information Technology, Institut Sains dan Teknologi Annuqayah, Sumenep, Indonesia*
[b] *Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia*
[c] *Department of Business Information Technology, College of Business and Economics, University of Rwanda, Kigali, Rwanda*
[d] *Department of Computer Science and Information Technology, La Trobe University, Melbourne, Australia*
[e] *Department of Data Science and AI, Monash University, Melbourne, Australia*
Corresponding author: [*]tohari@if.its.ac.id

***Abstract*— For some periods, information technology has developed, but there are some issues with its data security. For this reason, exploring the data hiding method is relevant, which is an appropriate study in the information concealment paradigm. Several factors must be considered in its implementation, such as the capacity of the confidential data and the quality of the generated stego file. Nevertheless, it is difficult to solve those two problems simultaneously in actual application. We often need to choose either one of them, which is more suitable for a specific environment. In this research, those problems are approached by extending the Quad General Difference Expansion Cluster (QGDEC) method combined with fuzzy logic in the image environment. We use the cluster in the QGDEC, which aims to ensure that the pixel difference is not significant so that the quality of the stego can be maintained. The confidential data can be embedded in multiple layers based on several image characteristics, which can be processed using fuzzy logic. The result of the experiment denotes that the proposed method obtains about 20 dB higher than that of the previous ones regarding the Peak Signal to Noise Ratio (PSNR) for the same capacity of the secret. It depicts that the proposed method is more applicable than the previous ones by considering the specific message size and its respective characteristics.**

***Keywords*— Data hiding; information hiding; steganography; information security; network infrastructure.**

Manuscript received 9 Aug. 2021; revised 11 Jan. 2022; accepted 12 Apr. 2022. Date of publication 31 Dec. 2022.

I. INTRODUCTION

As a result of technological developments in network communication and information in this era, some security issues, such as identity theft and data misuse, arise due to unauthorized access to the systems [1], [2]. Therefore, it is crucial to design security techniques to protect information systems and preserve privacy to prevent illegal access [3], [4]. Along with encryption, a method has been developed to protect data, hiding confidential data in particular media. This technique is called steganography or data hiding.

Broadly speaking, data hiding is a security measure that is done by embedding those confidential data within specific media that are accessible by authorized users only. For this reason, this technique can be a solution to deal with data security problems. This technique also deceives a third party while the data are being transmitted, and it is because the sender is viewed as only sending regular files even though there is a hidden message. Various kinds of media can be explored, such as text, image [5], audio [6], and video [7].

Reversible Data Hiding (RDH) has become a potential topic to be applied. In its implementation, several factors must be considered to achieve its purpose. First, the medium embedded with confidential data (called stego) must be highly similar to the original medium (cover). Such a significant difference may cause the public to be suspicious of the file being transmitted. Second, a high embedding capacity shows that the technique is better because more data can be accommodated. Those factors can be explained as imperceptibility, fidelity, and recovery. Imperceptibility means that the appearance of confidential data cannot be detected by the human senses, whereas fidelity means that the media quality of the coverage has not changed dramatically because of the embedding. If its quality degrades, an attacker

may detect it as abnormal, which attracts him/her to intercept. Next, recovery means the confidential data can be reconstructed back to its original form.

Various techniques have been used to reach image reversibility. The application domain has become a basic technique that is often used to look for image reversibility. This technique can be classified extensively into transform (frequency) and spatial domain techniques [8]. In the spatial domain, changing pixel values from the cover image hides the secret message to gain the desirable enhancement directly. Meanwhile, the carrier medium is first mapped to the transform domain, and then the confidential data are concealed in that medium. Many studies take spatial domains, such as Difference Expansion (DE) [8], Histogram Shifting [9], encrypted image using Huffman coding [10], specific encryption [11], Most Significant Bit (MSB) [12], Prediction Error Expansion [13], adaptive MSB encoding [14], Pixel Prediction [15], and multi-layer embedding [16].

The development of steganography has been combined with intelligent algorithms, such as Fuzzy C-Means (FCM), Hybrid Neural Networks (HNN), K-nearest neighbors (KNN), and Decision Tree (DT). This composition aims to gain the best outcome and suitable solutions. Various improvements have been performed, like [17] that integrates Fuzzy Logic (FL) with RDE to specify embedding levels, and [18] that works on FL and LSB. However, this method still uses LSB to enter data so that the original images cannot be reconstructed. Ashraf et al. [19] propose an interval system based on type 2 fuzzy logic to find pixels in images that are less visible to the individual senses. Here, the LSB is taken for the embedding process. Hou et al. [20] implement a deep neural network for generating various histograms. It is intended to reduce the noise. Wang et al. [21] apply Fuzzy C-means (FCM) clustering to indicate the construction of multiple histograms. This FCM, designed with prediction errors, is applied to group the carrier (cover) into several clusters with similar characteristics. These patterns are subsequently utilized to develop multiple histograms for effective data insertion.

To overcome the data hiding reversibility problem, maintain the image quality, and increase the embedding capacity, we propose a technique by improving the Quad General Difference Expansion Cluster (QGDEC) and exploring fuzzy logic methods in the image environment. QGDEC is a development of the DE method that can increase the confidential data's capacity and reduce the distortion in the image. In other words, the QGDEC method can obtain a more negligible difference than the DE method. The QGDEC itself is a reversible data hiding method, which means the stego image generated from the QGDEC method can be returned to its original cover by going through the extraction process.

In this case, the fuzzy logic method dynamically specifies the maximum inserting level in the multiple-layer design. The block's level is determined by first extracting image characteristics, then a Fuzzy Inference System (FIS) process is carried out, and finally, the capacity of the secret can be estimated. The image characteristics to investigate are the median and the average of the difference from neighboring pixels, taking that of Tsai et al. [22], in which only left and uppermost side neighboring pixels are used. This research considers all the neighboring pixels in the 2×2 block.

The maximum embedding level of a block is defined as the highest layer for embedding the message. For example, from the fuzzy logic calculation, a block's maximum level of embedding is level four, and it means that the embedding can be performed up to four times.

The QGDEC is used for inserting secret bit messages based on the values obtained from the fuzzy process. Another goal is to avoid substantial differences between the new pixels of the stego and the cover image, which decreases the image quality. It is done by designing pixel clusters.

To support that method, some previous works have been reviewed. We find that one of the most popular reversible data hiding techniques is DE. It is to hide confidential data by employing differences between neighboring pairs of pixels. Furthermore, it is relatively simple to apply, and many studies have extended it to deliver better capacity and complexity aspects, including hardware [23].

Research in data hiding has been done intensively [5], [6], [24]. Puteaux et al. [5] conducted a research survey on data hiding in transformed images. Here, they find that the combination of data hiding and cryptography is popular for various reasons, such as the need for classified information, cloud storage, and digital right management. The schemes to implement include histogram shifting, pixel value ordering, prediction-based, and partition-based. They infer that most algorithms work well either on the payload capacity or the quality, considering that it is hard to increase both factors concurrently.

Maniriho and Ahmad [8] also apply DE to improve information hiding, combining it with the modulus function. This scheme prevents a decrease in embedding capacity by considering the value of positive and negative differences to hide confidential data. The experimental results show that this scheme performs better than the existing methods. Muttaqi and Ahmad [25] improve the method proposed in Maniriho and Ahmad [8] by combining a modulus function and RDE for low difference pixel values of an adjacent pixel with 2×1 blocks size. They use RDE to reduce high pixel values. The variations of DE, such as the difference expansion of quad and multiple layer hiding, are described as follows.

A. Difference Expansion of Quad

Initially, Alattar [26] has proposed the Difference Expansion of Quad, which develops the difference expansion method. In this method, the carrier is split into 2×2 blocks, each of which comprises four pixels.

For every block $p = (p_1, p_2, p_3, p_4)$, that scheme [26] describes the difference value among the vector p as in Eq. (1).

$$\begin{cases} v_1 = p_1 - p_0 \\ v_2 = p_2 - p_1 \\ v_3 = p_3 - p_2 \end{cases} \quad (1)$$

Next, Eq. (2), which is the inverse of Eq. (1), is used to reconstruct the original carrier.

$$\begin{cases} p_1 = v_0 - \left\lfloor \frac{3v_1 + 2v_2 + v_3}{4} \right\rfloor \\ p_2 = v_1 + p_0 \\ p_3 = v_2 + p_1 \\ p_4 = v_3 + p_2 \end{cases} \quad (2)$$

For the data bit b_i, insertion is implemented using two options as provided in either Eq. (3) or Eq. (4). First, the pixels block is inserted by using Eq. (3). Furthermore, it is labeled as expandable. The embedding process is changed to Eq. (4) and labeled as changeable in the matter of overflow or underflow. Finally, blocks are labeled as unchangeable if not included in the second category.

$$\begin{cases} \tilde{v}_1 = 2 \times v_1 + b_1 \\ \tilde{v}_2 = 2 \times v_2 + b_2 \\ \tilde{v}_3 = 2 \times v_3 + b_3 \end{cases} \quad (3)$$

$$\begin{cases} \tilde{v}_1 = 2 \times \frac{v_1}{2} + b_1 \\ \tilde{v}_2 = 2 \times \frac{v_2}{2} + b_2 \\ \tilde{v}_3 = 2 \times \frac{v_3}{2} + b_3 \end{cases} \quad (4)$$

To prevent both underflow and overflow, the difference pixel value that has been inserted by confidential messages must meet Eq. (5). Afterward, the new pixel $\tilde{p}_i$ is determined by Eq. (6). With this method, the highest hiding capacity is 0.75 bits per pixel (bpp).

$$\begin{cases} 0 \le v_0 - \left\lfloor \frac{v_1+v_2+v_3}{4} \right\rfloor \le 255 \\ 0 \le \tilde{v}_1 - p_0 \le 255 \\ 0 \le \tilde{v}_2 - p_1 \le 255 \\ 0 \le \tilde{v}_3 - p_2 \le 255 \end{cases} \quad (5)$$

$$\begin{cases} \tilde{p}_0 = p_0 \\ \tilde{p}_1 = \tilde{v}_1 + p_0 \\ \tilde{p}_1 = \tilde{v}_2 + p_1 \\ \tilde{p}_1 = \tilde{v}_3 + p_2 \end{cases} \quad (6)$$

B. Multiple layer embedding based on DE

The DE method is implemented to embed data several times. In the conventional DE method, embedding increases the difference in the pixel pairs' values. Underflow or overflow will occur in the next layer if multi-layer hiding is implemented in this DE scheme, decreasing image distortion and hiding capacity. Lou et al. [27] took the RDE to drop the differential expansion between the pixel blocks in every layer to overcome that issue.

Multi-layer insertion starts by scanning horizontally to obtain the pixel pairs in the first layer. Then the pair is scanned again using vertical scanning for the next layer. Vertical and horizontal scanning are carried out alternately until layer k is completed, where k is the highest value of layers. In images whose size is m×n, the DE hiding space of this method is (m×n)/2 bits, while the multi-layer hiding capacity is (m×n/2×k) bits.

This paper is provided in four sections. Section 1 is the introduction along with the related studies to the proposed method, while the proposed method itself is explained in Section 2, and the experiment results are provided in Section 3. Lastly, the results are discussed and concluded in Section 4.

II. MATERIALS AND METHOD

This section explains the flow of the method, containing the design of the embedding and extracting processes. The total level of multi-layer embedding is investigated by looking at image characteristics. Furthermore, the embedding of secret messages is performed by exploring pixel clusters.

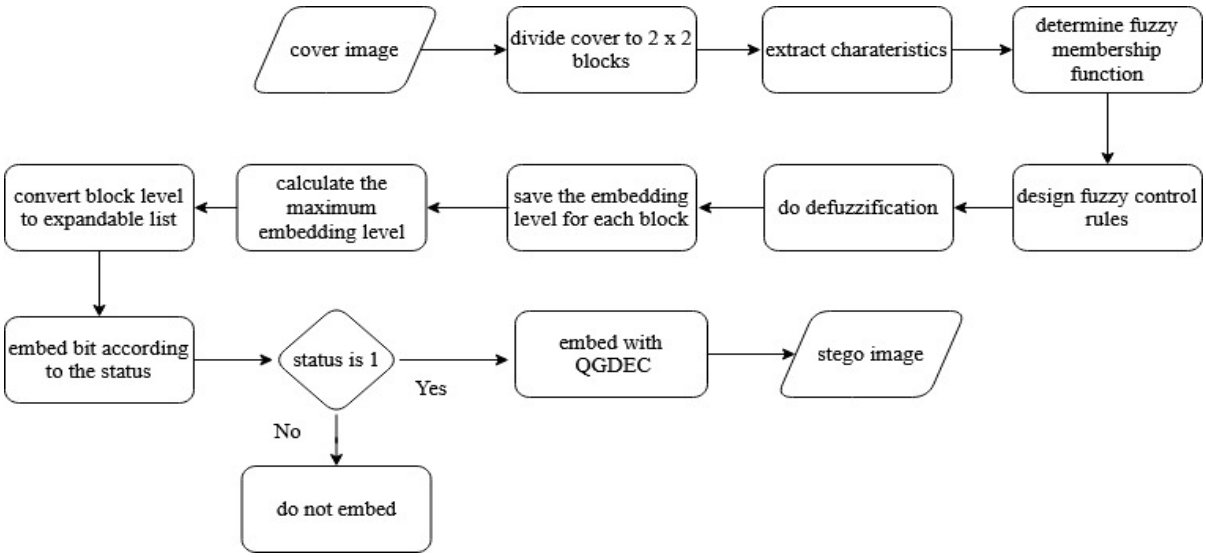


Fig. 1 Embedding process

A. General Description of the Method

The proposed development method specifies the embedding level by looking at image characteristics and embedding secret messages using pixel clusters. This embedding level is applied to the development of the DE, namely multi-layered QGDEC. The number of the embedding determines the highest number of layers embeddable into the block that, in this research, its size is 2×2 pixels.

The pixel cluster is performed to find the difference between the original carrier's pixel values with the lowest or uppermost limit of the cluster, where the pixel value of the original image is located. So, it is expected that the pixel cluster can avoid significant differences that can affect massive changes in the pixel value of stego images. The image quality can likely be maintained even though it has

been inserted by a secret message. Each block has a different embedding level, calculated for the corresponding block using fuzzy logic. For this purpose, the characteristics of images are investigated.

B. Overall Scheme

The beginning step in this proposed method is inspired by the adaptive steganography scheme developed based on the fuzzy inference system called FIS [18], [17]. However, the characteristics of the image used as fuzzy input are undoubtedly different. It is due to the different nature between LSB and DE embedding methods. So, this scheme's initial stage produces fuzzy inference systems different from those proposed in Sajasi et al. [18]. In comparison, image characteristics were used in the form of the average standard deviation, local distance, and entropy in one block [17]. We computed the averages and medians of the differences between neighboring pixels in a block.

This paper is inspired by Lou et al. [27], but it differs in how the scanning pixels are performed. Lout et al. [27] take 3×3 block sizes, whereas we calculate the difference between the original image pixels in the 2×2 block with the lowest and uppermost cluster range. Then the embedding is done using the QGDEC method per the embedding level of every block according to the process fuzzy logic method results. Fig. 1 illustrates this embedding process.

C. Design of the Embedding Level Mechanism

At the embedding stage, the image quality decreases according to the number of layers being applied, and the capacity increases.

1) Designing Fuzzy Variables: Unlike Ilham et al. [17], that takes standard deviations, brightness, local distances, and local entropy for the characteristics of fuzzy inputs, here we also investigate the average of the difference between the neighboring pixel values for each block. For this purpose, we determine Eq. (7) for finding the difference between neighboring pixels from the pixel value of each block.

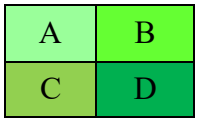


Fig. 2 Example of a pixel block

Fig. 2 illustrates the pixel block, whose difference h is calculated by using Eq. (7). It is then applied as a reference input to the fuzzy membership function by finding their average and median.

$$h = \{|A-B|, |B-C|, |A-C|, |A-D|, |B-D|, |C-D|\} \quad (7)$$

2) Fuzzification and Fuzzy Membership Function: We determine fuzzy membership functions from the characteristics of the predetermined block whose value is between 0 and 128, as shown in Table 1. The embedding level value has a universe whose domain is from 0 to 8, as described in Table 2, referring to the experiment of [14]. Furthermore, it is a fuzzy output. The research applies a trapezoidal curve in terms of fuzzy membership function, which has 4 points: *a*, *b*, *c*, and *d*. The minor domain is depicted by point *a*, which has zero membership, while point *b* shows the value of the smallest domain that has one member. Point *c* is the most substantial domain value with one membership degree, while the most significant domain is depicted by point *d*, which has zero membership.

TABLE I
FUZZY MEMBERSHIP FUNCTION

Point a	Point b	Point c	Point d	Linguistic Variable
-5.00	-1.00	0.00	1.00	Very small
0.50	1.00	9.50	10.50	Small
9.50	10.50	18.00	22.00	Small to medium
18.00	22.00	28.00	32.00	Medium to large
28.00	32.00	80.00	100.00	Large
80.00	100.00	128.0	140.0	Very large

TABLE II
THE OUTPUT OF THE FUZZY MEMBERSHIP FUNCTION

Point a	Point b	Point c	Point d	Linguistic Variable
-1.00	0	0.25	0.5	Very small
0.25	0.5	1.5	1.75	Smal
1.5	1.75	3	3.5	Small to moderate
3	3.5	5	5.5	Moderate to large
5	5.5	7	7.5	Large
7	7.75	8	9	Very large

TABLE III
FUZZY LOGIC CONTROLLER OF THE AVERAGE AND THE MEDIAN

Embedding Level	Average and Median of the Difference Pixel Neighboring					
	VS	S	STM	MTL	L	VL
	VL	L	MTL	STM	S	VS

3) Fuzzy Logic Controller: We use the Fuzzy logic controller, which is provided in Table 3. It shows linguistic values, namely: very small (VS), small (S), small to moderate (STM), moderate to large (MTL), large (L), and very large (VL).

4) Defuzzification: In this research, we use the centroid-based method, often called the Center of Gravity (COG) [28]. Since the fuzzing step's initial result can have a fractional value, it is necessary to round it up before being used as the embedding level value.

D. Bit Embedding and Bit Extraction

We extend QGDEC [29] to embed confidential data. Nevertheless, that method [29] only processes one layer and is only suitable for an image whose average pixel value is not more than 150. In other words, if the average pixel value is more than 150, the resulting stego image drops. To overcome this problem, we enhance [29] by adding the upper limit of the cluster.

E. Multi-layer Embedding Mechanism

In this mechanism, we develop an algorithm for scanning the blocks, the structure of the level, and location maps. For illustration, Fig. 3 presents the block structure, comprising pixel 1, pixel 2, pixel 3, and pixel 4. This data block is collected by scanning carrier images, whose order is depicted in Fig. 4, where scanning is performed horizontally. In that figure, the same number indicates pixels in the same block. This number is becoming the index pointer of the existing block.

This research uses a level map to save every block's embedding value, whose embedding level is determined by the appropriate characteristics. Next, the level map is built in the array format, where the column shows the index of a block. The number of blocks can be determined with (m×n)/4, where m×n is the image size. The illustration of this map is provided in Fig. 5.

An expandable blocklist is generated based on this level map in Fig. 5 (see Fig. 6). It is composed of a 2D array, where the column means the index of the block while the row shows the total layers in multi-layer insertion. In this case, the row value is 1 for embedding and 0 for otherwise. The number of rows with value one is generated from the maximum number of insertions, meaning that the number of rows with value 1 is equal to the maximum block level.

Like the RDE method in Ilham et al. [17], we also used location maps to ensure that the data have been processed correctly and that the method meets the reversibility. The structure of the location map is presented in Table 4.

F. The Embedding and Extraction with QGDEC

Unlike the DE method, which uses pixel pairs to look for pixel differences, the QGDEC method takes cluster pixels to find the pixel differences [29]. Then, these differences are reduced again to produce a smaller value.

1) Embedding Process: We designed a range of cluster pixels before carrying out the embedding scheme, as presented in Table 5. It is shown that the range of each cluster is 3. The implementation of this cluster is to control the stego image quality so that its quality does not suffer from significant deterioration.

The differences of d_i where $i \in \{1,2,3,4\}$, are obtained by reducing the original pixel image value with the lowest limit or the uppermost limit of the cluster range as in Eq. (8) and Eq. (9). K_b is the lowest limit of the cluster range, and K_a is the uppermost limit of the cluster range, whereas u is the pixel value of the original image. Eq. (8) is used when the average pixel value of the original image is less than or equal to 150, and Eq. (9) is if it is more than 150.

$$\left.\begin{aligned} d_1 &= u_1 - K_b \\ d_2 &= u_2 - K_b \\ d_3 &= u_3 - K_b \\ d_4 &= u_4 - K_b \end{aligned}\right\} \tag{8}$$

$$\left.\begin{aligned} d_1 &= K_a - u_1 \\ d_2 &= K_a - u_2 \\ d_3 &= K_a - u_3 \\ d_4 &= K_a - u_4 \end{aligned}\right\} \tag{9}$$

The next process is to reduce the value of d_i using Eq. (10).

$$d_i' = \begin{cases} 0 & , if\ d_i \le 2 \\ d_i - 2^{[Log_2 d_i]}, & if\ d_i = 3 \end{cases} \tag{10}$$

After getting the value of d_i', the next step is to insert a secret message (payload) using Eq. (11) to get the embedded difference d_i'', similar to the embedding process carried out in the RDE process. Next, the final process is to look for a new pixel value (stego pixel value) by using Eq. (12) or Eq. (13). As in the earlier case, Eq. (12) is taken if the average pixel value of the original image is not more than 150; otherwise, Eq. (13) is used. This QGDEC-based embedding process can be depicted in Fig. 7.

$$d_i'' = 2 \times d_i + b \tag{11}$$

$$\left.\begin{aligned} u_1' &= d"_1 + K_b \\ u_2' &= d"_2 + K_b \\ u_3' &= d"_3 + K_b \\ u_4' &= d"_4 + K_b \end{aligned}\right\} \tag{12}$$

$$\left.\begin{aligned} u_1' &= K_a - d"_1 \\ u_2' &= K_a - d"_2 \\ u_3' &= K_a - d"_3 \\ u_4' &= K_a - d"_4 \end{aligned}\right\} \tag{13}$$

1	2
3	4

Fig. 3 Structure of the block

1	1	2	2	3	3
1	1	2	2	3	3
4	4	5	5	6	6
4	4	5	5	6	6
7	7	8	8	9	9
7	7	8	8	9	9

Fig. 4 The sequence of the block scanning

2	3	1	0

Fig. 5 Example of the level map

1	1	1	0
1	1	0	0
0	1	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Fig. 6. List of the expandable block, according to the previous level map shown in Fig. 5

TABLE IV
LOCATION MAP

Value of d	Location Map Value
d = 0	00
d = 2	10
d = 1 or d = 3	11

TABLE V
CLUSTER OF PIXELS

Cluster	Range of Pixels	
	Lowest Limit	Uppermost Limit
K_1	0	3
K_2	4	7
K_3	8	11
…	…	…
K_{64}	252	255

2) Extraction Process: The complete extraction stages are as follows. Firstly, all pixel data from stego images are scanned. Second, the pixel value of the stego image is put into its cluster, as created in Table 5. Like the embedding process, the difference d_i is calculated using Eq. (8) or Eq. (9). Next, the secret data are extracted using Eq. (14). The reduction value is calculated to get the value of d_i' by using Eq. (15). After that, the value of d_i' is processed using Eq. (16) by adjusting the value of the Location Map. Lastly, the original pixels are calculated using the previous Eq. (11) or Eq. (12). Additionally, Fig. 8 demonstrates how the concealment and extraction stages are implemented, remembering the cover image and secret message to be embedded.

$$b = LSB(d_i) \tag{14}$$

$$d_i' = \left\lfloor \frac{d_i}{2} \right\rfloor \tag{15}$$

$$d_i'' = \begin{cases} 0 & ,if\ LM = 00 \\ d_i' + 2^{log_2\lfloor(2 \times d')+1\rfloor} + 1 & ,if\ LM = 10 \\ d_i' + 2^{log_2\lfloor(2 \times d')+1\rfloor} & ,if\ LM = 11 \end{cases} \tag{16}$$

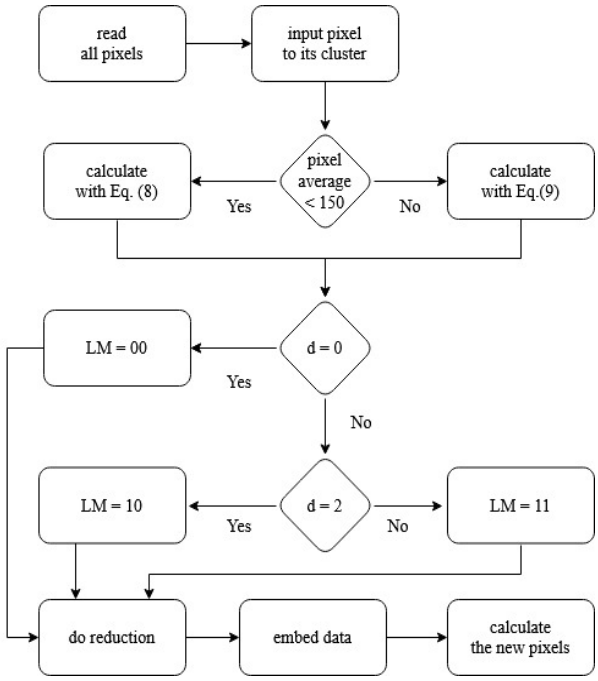


Fig. 7 The process of embedding data with QGDEC

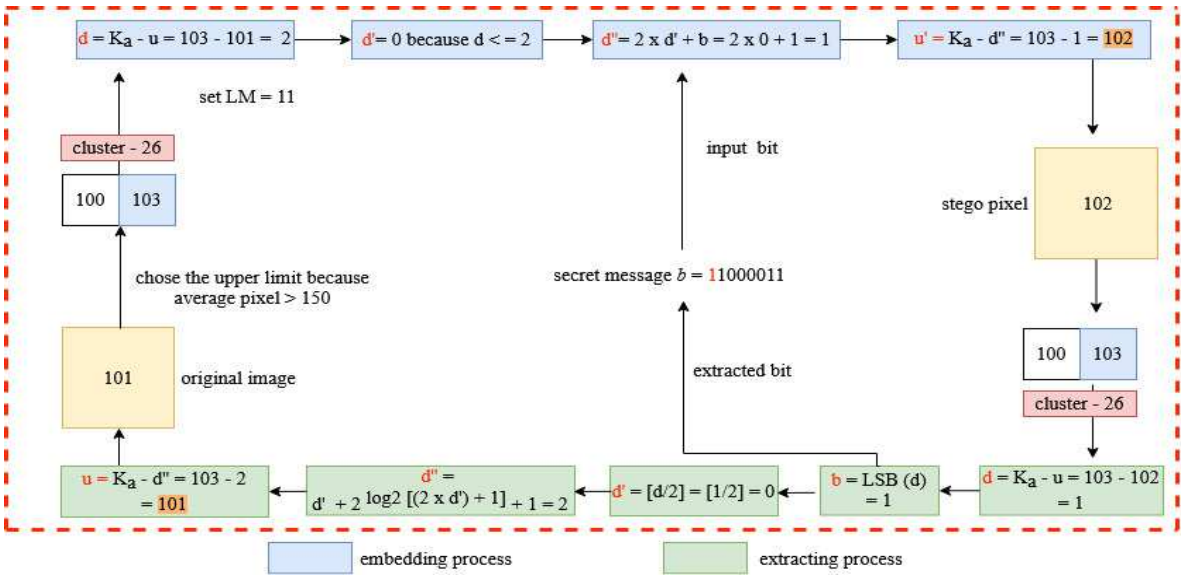
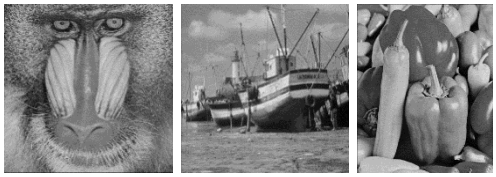


Fig. 8 Example of the insertion and extraction

III. RESULT AND DISCUSSION

Several scenarios and testing images are needed to assess the proposed method. This research applies six standard grayscale images [30], [31], which size is 512×512 pixels. Examples of them are depicted in Fig. 9.



(a). (b). (c).

Fig. 9. Examples of standard images for the experiment [30][31]. (a) Baboon. (b). Boat (c) Peppers

The experiment evaluates the image's quality after the embedding process. If the stego image is more similar to the cover image, then the proposed method is better. We use the Peak Signal to Noise Ratio (PSNR) value to measure the similarity between the cover and stego images. The PSNR value itself is described as in Eq. (17).

$$\begin{cases} PSNR = 10\log_{10}\frac{255^2}{MSE} \\ MSE = \frac{1}{Hx\,W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(Y_{ij} - Y'_{ij}\right)^2 \end{cases} \quad (17)$$

MSE is the mean square error representing the difference between the stego Y' and the original image Y. The higher the PSNR value, the higher the similarity between the stego image and the cover image. In other words, a higher PSNR value indicates a better result.

We determine the stego image quality by embedding payloads from 10 kb to 70 kb, compared with that of three other methods. The first comparison is made with Muttaqi and Ahmad [25] that used a modulus function and RDE, and its result is presented in Table 6. The second is done with the method proposed by Ilham et al.'s works [17] that used fuzzy logic and RDE methods for multi-layer embedding, provided in Table 7. Next, Table 8 exposes the comparison between Lou et al.'s [27] and the proposed method.

TABLE VI
COMPARISON OF PSNR VALUE BETWEEN MUTTAQI AND AHMAD [25] AND THE PROPOSED METHOD

		PSNR (dB)						
Cover	**Method**	**10kb**	**20kb**	**30kb**	**40kb**	**50kb**	**60kb**	**70kb**
Fruits	Muttaqi and Ahmad [25]	48.63	45.33	43.59	42.26	41.31	40.87	40.04
	Proposed	66.30	63.02	61.30	60.09	59.08	58.64	57.67
Airplane	Muttaqi and Ahmad [25]	57.54	54.71	53.17	51.79	50.37	49.15	47.03
	Proposed	64.89	62.17	60.49	59.33	58.48	57.99	57.14
Boat	Muttaqi and Ahmad [25]	53.36	49.82	47.45	45.57	44.05	43.37	42.03
	Proposed	65.63	62.57	60.82	59.61	58.68	58.17	57.17
Baboon	Muttaqi and Ahmad [25]	45.38	43.05	41.37	40.51	39.93	39.67	39.11
	Proposed	61.65	58.62	56.99	55.89	55.19	54.85	54.19
Peppers	Muttaqi and Ahmad [25]	53.72	50.73	48.98	47.48	46.45	45.97	44.77
	Proposed	64.85	62.25	60.65	59.46	58.55	57.96	56.99
Car	Muttaqi and Ahmad [25]	54.34	50.22	47.71	45.61	44.19	43.47	41.90
	Proposed	65.82	62.76	61.12	59.94	59.09	58.62	57.66

TABLE VII
COMPARISON OF PSNR VALUE BETWEEN ILHAM ET AL. [17] AND THE PROPOSED METHOD

		PSNR (dB)						
Cover	**Method**	**10kb**	**20kb**	**30kb**	**40kb**	**50kb**	**60kb**	**70kb**
Fruits	Ilham et al. [17]	51.06	47.84	45.63	44.38	43.42	42.53	40.98
	Proposed	66.30	63.02	61.30	60.09	59.08	58.64	57.67
Airplane	Ilham et al. [17]	55.66	51.85	49.79	48.45	47.41	46.32	45.26
	Proposed	64.89	62.17	60.49	59.33	58.48	57.99	57.14
Boat	Ilham et al. [17]	54.70	50.64	48.63	46.69	44.93	43.92	42.94
	Proposed	65.63	62.57	60.82	59.61	58.68	58.17	57.17
Baboon	Ilham et al. [17]	45.81	43.45	42.02	41.92	40.81	39.84	38.34
	Proposed	61.65	58.62	56.99	55.89	55.19	54.85	54.19
Peppers	Ilham et al. [17]	55.67	51.92	49.74	48.43	47.33	46.32	45.22
	Proposed	64.85	62.25	60.65	59.46	58.55	57.96	56.99
Car	Ilham et al. [17]	55.87	53.74	51.53	49.65	47.92	46.53	45.34
	Proposed	65.82	62.76	61.12	59.94	59.09	58.62	57.66

Also, we measured the embedded data's capacity to find the maximum number of bits that can be embedded in the cover image. As in the previous scenario, it is also compared with those three existing methods. It explores whether alterations in image quality will affect data embedding capacity, as shown in Table 9.

Tables 6, 7, and 8 show that the proposed scheme achieved the best PSNR results compared to the others, which reached the highest PSNR value of 66.30 dB for typical image 'Fruits'. Furthermore, Ilham et al.'s method have a better PSNR value than both methods, which reached the highest PSNR value of 55.87 dB for the basic image 'Car'. Table 9 shows that the proposed method has a smaller embedding capacity than Lou et al.'s and slightly below Ilham et al.'s. It happens because, in general, increasing message size leads to reducing PSNR values. Despite this trade-off, in some cases, increasing the quality of the stego image may be harder than raising the capacity, depending on the characteristics of the cover that have been investigated in this research. Nevertheless, at the implementation level, what factor to consider, whether the quality or the capacity, depends on the required purpose of the interconnected system.

TABLE VIII
COMPARISON OF PSNR VALUE BETWEEN LOU ET AL. [27] AND THE PROPOSED METHOD

		PSNR (dB)						
Cover	**Method**	**10kb**	**20kb**	**30kb**	**40kb**	**50kb**	**60kb**	**70kb**
Fruits	Lou et al. [27]	45.51	41.88	40.22	39.12	38.23	37.83	37.16
	Proposed	66.30	63.02	61.30	60.09	59.08	58.64	57.67
Airplane	Lou et al. [27]	53.63	49.81	47.11	45.03	43.47	42.39	40.97
	Proposed	64.89	62.17	60.49	59.33	58.48	57.99	57.14
Boat	Lou et al. [27]	53.82	49.99	47.37	45.34	43.86	42.73	41.25
	Proposed	65.63	62.57	60.82	59.61	58.68	58.17	57.17
Baboon	Lou et al. [27]	44.47	42.35	40.87	40.23	39.83	37.82	36.27
	Proposed	61.65	58.62	56.99	55.89	55.19	54.85	54.19
Peppers	Lou et al. [27]	55.13	51.62	49.42	48.03	47.03	46.03	44.92
	Proposed	64.85	62.25	60.65	59.46	58.55	57.96	56.99
Car	Lou et al. [27]	53.22	49.98	47.80	46.02	44.63	43.94	42.11
	Proposed	65.82	62.76	61.12	59.94	59.09	58.62	57.66

TABLE IX
COMPARISON OF THE MAXIMUM EMBEDDING CAPACITY

	Capacity (bits)			
Cover	**Muttaqi and Ahmad [25]**	**Ilham et al. [17]**	**Lou et al. [27]**	**Proposed Method**
Fruits	128.971	670.600	1.025.432	624.390
Airplane	131.072	710.960	1.010.463	700.690
Boat	130.808	712.878	1.010.556	701.843
Baboon	131.061	777.892	1.028.764	768.298
Peppers	130.780	513.586	953.932	502.983
Car	130.871	711.924	1.010.920	701.742

IV. CONCLUSION

This paper uses fuzzy logic to determine the embedding level based on several image characteristics, such as the average and median of the difference between neighboring pixels. We have also extended the QGDEC method to increase the value of PSNR in embedding secret messages into the carrier image.

We evaluated the proposed method in terms of capacity and PSNR. In terms of PSNR, the result of the experiment denotes that the proposed method obtains a highly better value than the existing method. It is shown that the difference between the stego image and the cover image can be reduced with the use of clusters. In other cases, the proposed method has a smaller capacity than Lou's and Ilham's. It is because Lou's method directly embeds confidential data into the cover image without first paying attention to the image characteristics. However, as presented in the experiment results, further development in the value of the PSNR and embedding capacity is still needed in future work.

REFERENCES

[1] G. Zhang, Z. Yang, H. Xie, and W. Liu, "A secure authorized deduplication scheme for cloud data based on blockchain," *Inf. Process. Manag.*, vol. 58, no. 3, p. 102510, 2021, doi: 10.1016/j.ipm.2021.102510.

[2] A. A. Gutub and K. A. Alaseri, "Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing," *J. King Saud Univ. - Comput. Inf. Sci.*, no. in press, Available online 28 June 2019, 2019, doi: 10.1016/j.jksuci.2019.06.014.

[3] H. Agrawal and A. A. Agarkar, "LRSPPP: lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid," *Heliyon*, vol. 5(3), 2019, doi: 10.1504/IJICS.2019.10019163.

[4] M. Wrzeszcz, Ł. Dutka, R. G. Słota, and J. Kitowski, "New approach to global data access in computational infrastructures," *Futur. Gener. Comput. Syst.*, vol. 125, pp. 575–589, 2021, doi: 10.1016/j.future.2021.06.054.

[5] P. Puteaux, S. Y. Ong, K. S. Wong, and W. Puech, "A survey of reversible data hiding in encrypted images – The first 12 years," *J. Vis. Commun. Image Represent.*, vol. 77, no. September 2020, p. 103085, 2021, doi: 10.1016/j.jvcir.2021.103085.

[6] A. A. Alsabhany, A. H. Ali, F. Ridzuan, A. H. Azni, and M. R. Mokhtar, "Digital audio steganography: Systematic review, classification, and analysis of the current state of the art," *Comput. Sci. Rev.*, vol. 38, p. 100316, 2020, doi: 10.1016/j.cosrev.2020.100316.

[7] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," *Neurocomputing*, vol. 335, pp. 238–250, 2019, doi: 10.1016/j.neucom.2018.09.091.

[8] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 31, no. 3, pp. 335–347, 2019, doi: 10.1016/j.jksuci.2018.01.011.

[9] F. R. Shareef, "A novel crypto technique based ciphertext shifting," *Egypt. Informatics J.*, vol. 21, no. 2, pp. 83–90, 2020, doi: 10.1016/j.eij.2019.11.002.

[10] 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, no. January 2020, p. 103060, 2021, doi: 10.1016/j.jvcir.2021.103060.

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

[12] B. Guan and D. Xu, "An efficient high-capacity reversible data hiding scheme for encrypted images," *J. Vis. Commun. Image Represent.*, vol. 66, p. 102744, 2020, doi: 10.1016/j.jvcir.2019.102744.

[13] S. Yi, Y. Zhou, and Z. Hua, "Signal Processing : Image Communication Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion," *Signal Process. Image Commun.*, vol. 64, no. March, pp. 78–88, 2018, doi: 10.1016/j.image.2018.03.001.

[14] X. Wang, C. C. Chang, and C. C. Lin, "Reversible data hiding in encrypted images with block-based adaptive MSB encoding," *Inf. Sci. (Ny).*, vol. 567, pp. 375–394, 2021, doi: 10.1016/j.ins.2021.02.079.

[15] H. Ren, W. Lu, and B. Chen, "Reversible data hiding in encrypted binary images by pixel prediction," *Signal Processing*, vol. 165, pp. 268–277, 2019, doi: 10.1016/j.sigpro.2019.07.020.

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

[17] A. J. Ilham, P. H. Bawa, and T. Ahmad, "Protecting Secret Data using RDE and Fuzzy Logic to Specify the Embedding Level," *Proc. 2019 IEEE Int. Conf. Signal Image Process. Appl.*, vol. 19, pp. 254–258, 2019, doi: https://doi.org/10.1109/ICSIPA45851.2019.8977778.

[18] S. Sajasi, A. Masoud, and E. Moghadam, "A High Quality Image Steganography Scheme Based on Fuzzy Inference System," *2013 13th Iran. Conf. Fuzzy Syst.*, pp. 1–6, 2013, doi: 10.1109/IFSC.2013.6675666.

[19] Z. Ashraf, M. L. Roy, P. K. Muhuri, and Q. M. D. Lohani, "A Novel Image Steganography Approach Based on Interval Type-2 Fuzzy Similarity," *2018 IEEE Int. Conf. Fuzzy Syst.*, vol. 18, pp. 1–8, 2018, doi: https://doi.org/10.1109/FUZZ-IEEE.2018.8491582.

[20] J. Hou, B. Ou, H. Tian, and Z. Qin, "Reversible data hiding based on multiple histograms modification and deep neural networks," *Signal Process. Image Commun.*, vol. 92, no. December 2020, 2021, doi: 10.1016/j.image.2020.116118.

[21] J. Wang, N. Mao, X. Chen, J. Ni, and C. Wang, "Multiple histograms based reversible data hiding by using FCM clustering," *Signal Processing*, vol. 159, pp. 193–203, 2019, doi: 10.1016/j.sigpro.2019.02.013.

[22] Y. Tsai, D. Tsai, and C. Liu, "Reversible data hiding scheme based on neighboring pixel differences," *Digit. Signal Process.*, vol. 23, no. 3, pp. 919–927, 2013, doi: 10.1016/j.dsp.2012.12.014.

[23] S. Das, A. K. Sunaniya, R. Maity, and N. P. Maity, "Efficient FPGA implementation and verification of difference expansion based reversible watermarking with improved time and resource utilization," *Microprocess. Microsyst.*, vol. 83, no. December 2020, p. 103732, 2021, doi: 10.1016/j.micpro.2020.103732.

[24] 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, 2019, doi: 10.1016/j.neucom.2018.06.075.

[25] S. R. Muttaqi and T. Ahmad, "A new data hiding method for protecting bigger secret data," 2019, doi: 10.1109/ICTS.2019.8850938.

[26] A. M. Alattar, "Reversible watermark using difference expansion of quads," *IEEE Int. Conf. Acoust. Speech, Signal Process.*, vol. 3, no. 1, pp. 377–380, 2004, doi: 10.1109/ICASSP.2004.1326560.

[27] D. Lou, M. Hu, and J. Liu, "Multiple layer data hiding scheme for medical images," *Comput. Stand. Interfaces*, vol. 31, pp. 329–335, 2009, doi: 10.1016/j.csi.2008.05.009.

[28] X. Yuan, Z. Liu, and E. S. Lee, "Center-of-gravity fuzzy systems based on normal fuzzy implications," *Comput. Math. with Appl.*, vol. 61, no. 9, pp. 2879–2898, 2011, doi: 10.1016/j.camwa.2011.03.074.

[29] A. P. Rahardjo, "Penggunaan Klaster Piksel untuk Meningkatkan Kinerja Reduced Difference Expansion (The Use of Pixel Clusters to Improve the Performance of Reduced Difference Expansion)," Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia, 2014.

[30] EMICROBES digital library - home. [Online]. Available: https://www.idimages.org/Default.aspx. [Accessed: 10-Jun-2021].

[31] The USC-SIPI Image Database. [Online]. Available: https://sipi.usc.edu/database/. [Accessed: 10-Jun-2021].