Digital Image Information Hiding Methods for Protecting Transmitted Data: A Survey

Pascal Maniriho and Tohari Ahmad
Department of Informatics, Institut Teknologi Sepuluh Nopember, Kampus ITS, Surabaya, 60111, Indonesia
Email: manpasco1@yahoo.com, tohari@if.its.ac.id

Abstract —The increased availability of the internet and massive growth of new communication technologies have made data transmission much easier. However, the security threats and vulnerabilities launched against the internet channel hinder this communication which ends up by making data available to the unauthorized users. Information hiding is one of the techniques to overcome this severe challenge. The process of concealing confidential data into multimedia carriers such as text, audio, image, and video refers to information (or data) hiding. Its main purpose is to protect data while disguising the presence of the hidden data and communication itself which keeps user privacy, data confidentiality, integrity and copyright protection since information sharing is kept confidential. Digital images are one the most popular multimedia carriers that are used in information hiding due to their pervasiveness and high redundancy. Hence, this paper presents a valuable survey on the existing digital image information hiding approaches developed using difference expansion (DE) and pixel value modification (PVM) techniques. Besides, fundamental concepts, illustrations and analysis on the performance of all methods reviewed coupled with the current trends on digital image information hiding are also presented so as to identify new direction for feature research.

Index Terms—Confidential data, data protection, data transmission, information hiding, information security

I. Introduction

Securing data has become among the top priorities in this highly modernized world where new technologies are evolved daily. The protection of data needs to be enforced in order to ensure that confidential data are only available to the authorized personnel. That is, the communication between the sender and the receiver must be kept private to prevent data being shared from any sort of malicious acts or operations. This allows the same data to be received as they were transferred by the sender which results in authentic communication. Cryptography is one the security defense mechanisms which have been around for several years. Cryptography is mainly based on two concepts namely: encryption and decryption. Encryption is employed to encode confidential data into a meaningless form while decryption is applied to decode the encoded data into its original form after reaching the destination. One of the limitations of cryptography is that the encrypted data can always be seen during the transmission which may attract malevolent users to go for further investigation which may lead to its damage or alteration [1].

Information (data) hiding is another security technique that conceals confidential information into innocuous multimedia cover media such as audio, text, image and video without disclosing the communication and the presence of the embedded data. That is, only slight modifications are made in the cover media to avoid suspicions that may arouse the sophisticated attackers who might have seen same cover media before [2]. Hence, the original properties of the cover media must always be maintained after concealing data. The advantage of information hiding over cryptography is its potential to mislead the public by completely disguising the existence of communication. Additionally, its application enhances the reliability and security of data transmission.

In the recent years, various information hiding models based on digital image have been already presented in the literature and two main categories specifically irreversible and reversible models are identified. In irreversible models, only the embedded confidential data can be retrieved after extraction whereas in reversible models both similar original cover media and the embedded data can be recovered. Moreover, based on the techniques that are employed to develop the models elucidated above, further five sub categories, i.e., Difference Expansion (DE) [3]-[6], Pixel Value Modification (PVM) [7], integer-to-integer transform [8], [9], Histogram Shifting (HS) [10], [11], Prediction Error Expansion (PEE) [12], [13], and lossless compression [1], [14], [15] are also identified.

Difference expansion and pixel value modification are among the most famous reversible data hiding techniques owing to their abilities to rebuild the identical original cover media after extracting the embedded data. Moreover, in sensitive situations such as forensic images, military image processing, remote sensing, medical diagnose, law enforcement and information security, Reversible Data Hiding (RDH) models become very effective for copyright and integrity protection where recovering the original cover media from the stego media is performed without any deformation. Vleeschouwe et al.'s work [16] presents an example of a family doctor image which is compressed and transmitted while

Manuscript received May 10, 2018; revised December 20, 2018.
This work was supported by Ministry of Research, Technology, Higher Education, Republic of Indonesia and ITS.
Corresponding author email: tohari@if.its.ac.id.
doi:10.12720/jcm.14.1.9-16

keeping hidden management information intact. In reversible data hiding confidential data should be concealed in way that preserves the visual quality of the cover image. To decrease changes or modifications that occur in the cover image while concealing data is one of the matter of utmost concerns in the field of information hiding. This paper presents a survey on the existing DE, Reduced Difference Expansion (RDE), PVM techniques and their performance analysis in terms of visual quality and embedding capacity that can be accommodated by the cover image. more importantly, strengths and weaknesses are also elaborated in order to give key motivations for the future researchers who might be interested in the field of information hiding.

The rest of this paper is organized as follows. Section 2 introduces fundamental concepts on digital information hiding. Section 3 presents the application of information hiding while Section 4 discusses information hiding in the spatial domain approach. The discussion on the existing DE, RDE and PVM techniques and summary on their overall performance are given in section 5. Finally, Section 6 draws conclusion on this work.

II. Fundemental Concepts

This section elaborates some of the basic concepts coupled with technical terms used in information hiding.

- Cover (or carrier) image: It refers to the image that carries the hidden data.
- Embedding capacity: This is the number of bits that can be concealed in the cover image without causing much deformation. It can be represented in the form of bits, kilobits or bits per pixel (bpp).
- Stego image: Denotes the image obtained after concealing the confidential data.
- Imperceptibility: It means that severe deformations should not occur in the cover image after concealing data. That is, embedding the secret data must not drastically change the statistical properties of the original cover image.

Furthermore, the robustness and security are also the conspicuous factors to be considered in digital image information hiding.

- Robustness: It shows the amount of alteration that the stego image can resist before the concealed information can be intercepted or destroyed by an adversary.
- Security: The inability of adversaries to detect the secret information.

Generally, Fig. 1 depicts the well-known research areas in the paradigm of information hiding as it is illustrated in Fig. 2, the digital image information hiding can be broadly categorized into spatial domain, frequency domain, transform domain, spread spectrum and model based approaches [17].

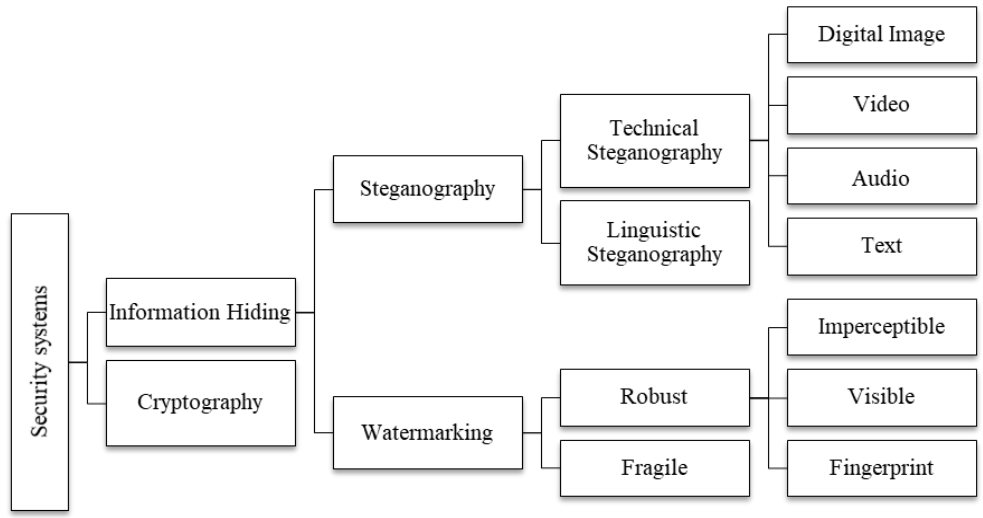

Fig. 1. Information hiding discipline

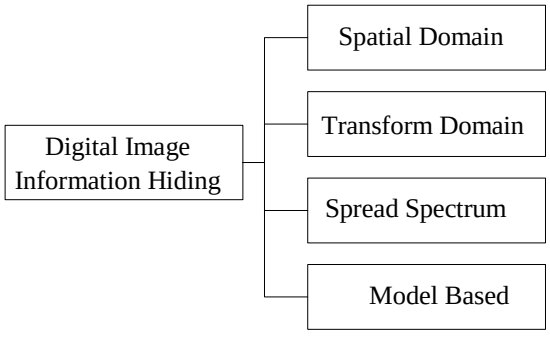

Fig. 2. Digital image steganography approaches

III. Digital Image Information Hiding In The Spatial Domain

In the spatial domain, the embedding is done by immediately concealing the secret data in the image pixel's value, i.e., the embedding is performed at the LSB level. The illustration of digital image steganography in the spatial domain can be viewed from Fig. 3. In addition, in order to demonstrate this concept, Fig. 4 depicts the whole process where the embedding is done by performing LSB substitution. Note that the substitution

occurs only from the first LSB till the fourth LSB. At the first stage, the embedding begins by first substituting the first LSB of the pixel value for the bit of the secret message and then the same process continues to the second, third till the forth LSB is also substituted. It is also important to mention that many modified LBSs will cause a drastic distortion of the stego image and as the results, adversaries can easily suspect the existence of the hidden message which is undesirable while sharing sensitive information.

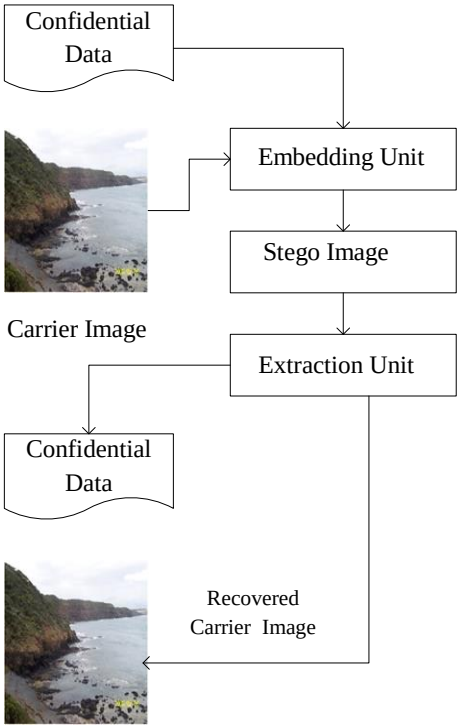

Fig. 3. Architecture of image steganography in the spatial domain

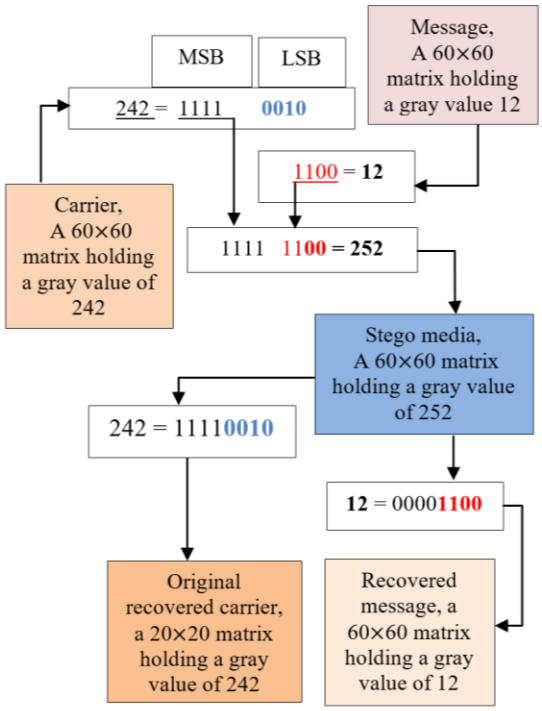

Fig. 4. The image steganography in the spatial domain [26]

IV. Discussion on DE and PVM Methods

A. Difference Expansion

The difference expansion is a data hiding technique that allows confidential data to be concealed in the difference values obtained after computing the difference between pixel pairs into the image. This technique has become more popular due to its simplicity and efficiency. Thereby, various DE-based methods already exist in the literature. In the work presented by Tian [3] in 2003, a difference expansion method was implemented. His work was considered as the building block for other DE information hiding methods, i.e., several DE methods were further implemented based on his work. Tian's DE method functionality can be summarized in the steps presented below. For a given cover image M, confidential data are concealed by:

The data embedding process starts with processing all pixels in a block. The steps are as follows:

1. First splitting up the cover image into blocks of size 2 by 1 (2×1), with two pixels $M_{1(i,j)}$ and $M_{2(i,j)}$ in each block where the subscripts (i, j) denote the position of the pixel in the image.
2. Calculate the difference between $M_{1(i,j)}$ and $M_{2(i,j)}$ and their respective average using the expression in (1) and (2). Note that the letter h is used to denotes the difference while y represents the average.

$$h = M_{1(i,j)} - M_{2(i,j)} \quad (1)$$

$$y = \frac{M_{1(i,j)} + M_{2(i,j)}}{2} \quad (2)$$

3. After generating all differences in each block, confidential data are concealed by extending them (h values) using (3) where h' is the extended difference having confidential data and s is the secret bit (0 or 1) which is hidden.

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

4. When the extension of the difference is completed, the next step is to compute the new pixels $M'_{1(i,j)}$ and $M'_{2(i,j)}$ which are further used to construct the stego image as shown in (4) and (5).

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

$$M'_{2(i,j)} = y - \left\lfloor \frac{h'}{2} \right\rfloor \quad (5)$$

5. Construct the stego image which can then be transmitted to the receiver over the public network. Moreover, to avoid the issue of overflow and underflow, the condition in (6) have to be evaluated. The first case (underflow) occurs when the pixel value is less than 0 ($M'_{1(i,j)}$ or $M'_{2(i,j)} < 0$); while for the second case (overflow) occurs when pixel value is greater 255 ($M'_{1(i,j)}$ or $M'_{2(i,j)} > 255$).

$$0 \le y + \left\lfloor \frac{h'+1}{2} \right\rfloor \le 255, \text{and } 0 \le y - \left\lfloor \frac{h'}{2} \right\rfloor \le 255 \quad (6)$$

Besides, Since Tian's method is totally reversible, in order to extract the hidden confidential data and recover the original cover image the extraction process is performed as follows. Similar to the concealment steps,

the same block size must be defined in the stego image.

1. Segment the stego image into blocks of size 2×1
2. Compute the difference and average between $M'_{1(i,j)}$ and $M'_{2(i,j)}$ using (7) and (8) respectively

$$h'' = M'_{1(i,j)} - M'_{2(i,j)} \tag{7}$$

$$y' = \frac{M'_{1(i,j)} + M'_{2(i,j)}}{2} \tag{8}$$

3. Recover the hidden confidential data using the expression provided in (9), i.e., the hidden bit s is extracted from the difference (h'')

$$s = LSB(h'') \tag{9}$$

4. Right shift the difference (h'') to recover the original one (h) by applying the expression in (10)

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

5. Recover the original pixels $M_{1(i,j)}$ and $M_{2(i,j)}$ using (11) and (12)

$$M_{1(i,j)} = y' + \left\lfloor \frac{h''+1}{2} \right\rfloor \tag{11}$$

$$M_{2(i,j)} = y' - \left\lfloor \frac{h''}{2} \right\rfloor \tag{12}$$

6. Reconstruct the original cover image by joining all recovered pixels → $M_{1(i,j)}$ and $M_{1(i,j)}$

It is worth to note that Tian's method has the capability to only hide one bit in each pair of pixels which does not cause underflow or overflow. That is, only those pixel pairs that fulfill the condition in (6) are modified otherwise they are kept unchanged.

B. Difference Expansion of Quad

According to Alattar [18], the embedding capacity and visual quality of the stego image can be significantly enhanced by increasing the size of the pixel block. Motivated by this concept, he proposed a difference expansion of quad to improve Tian's work [3]. A quad is block of pixels having four pixels which can be generated in the cover image by considering four pixels which are neighbors or randomly selecting them but the easiest way is to select those pixels which are neighbors. With reference to their findings, each quad has the ability to conceal 3 bits of the confidential data without greatly distorting the quality of the stego image. The overall operations of Alattar's approach is presented below.

The blocks of quad (blocks which have the size of 2 by 2→ (2×2) are first generated from the cover image by considering horizontal and vertical scanning. Once all blocks have been generated, pixels in each quad have to be arranged into vectors as it is presented in (13). For each quad (Q) the pixels' vector (Q_vector) is defined as $Q_{\_vec} = (Q_{0(i,j)}, Q_{1(i,j}, Q_{2(i,j)}, Q_{3(i,j)})$ thereafter the difference h is computed in each quad of vector in order to form the difference vector, $dif\_vect = (h_0, h_1, h_2, h_3)$ by applying (14).

$$Q_{\_vec} = (Q_{0(i,j)}, Q_{1(i,j}, Q_{2(i,j)}, Q_{3(i,j)}) \tag{13}$$

$$\begin{cases} h_o = \left\lfloor \frac{Q_{0(i,j)} + Q_{1(i,j)} + Q_{2(i,j)} + Q_{3(i,j)}}{4} \right\rfloor \\ h_1 = Q_{1(i,j)} - Q_{0(i,j)} \\ h_2 = Q_{2(i,j)} - Q_{1(i,j)} \\ h_3 = Q_{3(i,j)} - Q_{2(i,j)} \end{cases} \tag{14}$$

To conceal confidential data (s) which is represented in binary form, i.e., $s \rightarrow (0,1)$, the steps in (15) or (16) are executed.

a) Expanding the difference vector (dif_vect)

$$\begin{cases} h'_1 = 2 \times h_1 + s_1 \\ h'_2 = 2 \times h_2 + s_2 \\ h'_3 = 2 \times h_3 + s_3 \end{cases} \tag{15}$$

b) Performing LSB modification

$$\begin{cases} h'_1 = 2 \times \left\lfloor \frac{h_1}{2} \right\rfloor + s_1 \\ h'_2 = 2 \times \left\lfloor \frac{h_2}{2} \right\rfloor + s_2 \\ h'_3 = 2 \times \left\lfloor \frac{h_3}{2} \right\rfloor + s_2 \end{cases} \tag{16}$$

Notice that the expression in (15) is first applied to hide data, and if it happens that it causes underflow or overflow, the one in (16) is utilized. In case both of them are not suitable, no confidential data concealed in those blocks. Furthermore, the bits of the confidential data to be concealed are denoted by s_1, s_2, s_3 with all belonging to the set $s_n = \{0,1\}$. After concealing confidential data, the new pixel to be used to generate the stego image is built by adding up $dif_{vect} = (h'_o, h'_1, h'_2, h'_3)$ to the original pixel values $Q_{0(i,j)}, Q_{1(i,j}, Q_{2(i,j)}, Q_{3(i,j)}$ using (17). The output is the stego quad vector having pixels $(Q'_{0(i,j)}, Q'_{1(i,j}, Q'_{2(i,j)}, Q'_{3(i,j)})$, i.e., the block (Quad) Q is replaced by the new one (Q') containing the bits of the secret data in the stego image.

$$\begin{cases} Q'_{0(i,j)} = v'_0 - \left\lfloor \frac{Q_{0(i,j)} + Q_{1(i,j)} + Q_{2(i,j)} + Q_{3(i,j)}}{4} \right\rfloor \\ Q'_{1(i,j)} = v'_1 + Q'_{0(i,j)} \\ Q'_{2(i,j)} = v'_2 + Q'_{1(i,j)} \\ Q'_{3(i,j)} = v'_3 + Q'_{2(i,j)} \end{cases} \tag{17}$$

Two categories of block are defined. If the confidential data are concealed using (15) the quad is recorded as expandable while if it is performed using (16), the quad is recorded as changeable and if neither (15) nor (16) is used, the pixels in those quads are kept unchanged. These types of quad can be viewed in Fig. 5 and more details about this method can be found in [18].

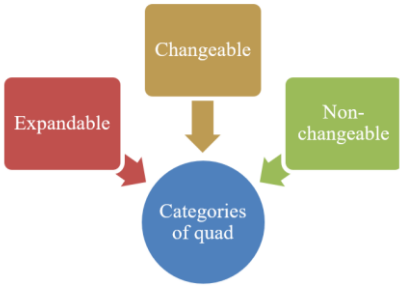

Fig. 5. Categories of quad [18]

C. Enhanced DE-with Controlled Expansion

In 2016, Angreni and Ahmad [19] proposed a new reversible data hiding method which is able to embed confidential data by expanding each pixel of the cover image, i.e., data can be embedded in all pixels by expanding them. Furthermore, their method solves the issue of underflow and overflow as well. New conditions and expressions for embedding and extracting data were also introduced in order to improve the performance of the previous methods. Besides, the extraction of the hidden data and the recovery of the cover image were carried out using the location map defined during the embedding process.

D. Centralized Difference Expansion

To decrease the degradation of the stego image while maintaining a high embedding capacity, a centralized difference expansion that employs a block-based lossless data embedding scheme was implemented by Lee et al. [20]. The size of data to be embedded highly depends on the type of the pixel block. Moreover, more secret bits are accommodated in blocks which have several smooth areas while for those blocks having few smooth areas, few secret bits are concealed. This makes the number secret bits to vary based on the nature of the cover image. That is, some cover images are characterized by a high redundancy allowing them to have several smooth areas suitable for concealing many secret bits while others can only hide few bits. In addition, different thresholds were used to identify the types of the block. Details on the reversibility of Lee et al.'s centralized RDH method are provided in [20].

E. Reduced Difference Expansion

After realizing that the difference expansion methods can sometimes cause underflow or overflow due to the large difference values that are added up to the pixels values which results in decreasing the payload capacity, a new data hiding technique namely, reduced difference expansion (RDE) was further introduced to remove the aforementioned drawbacks encountered in DE approach. Therein, various RDE methods have been already developed. The main steps to go through while applying RDE method are provided in Fig. 6. The work presented by Lu *et al.* [21] demonstrates that reducing the difference values increases the embedding capacity while preserving the quality of the stego image. The expression in (18) is the reduction scheme provided in Lu et al.'s work to reduce the difference values before concealing secret data.

$$h'_n = \begin{cases} h_n & \text{if } h_n < 2 \\ h_n - 2^{\lfloor log_2 h_n \rfloor - 1} & \text{otherwise} \end{cases} \quad (18)$$

For all difference values (h_n) which are equals to 1 or 0, → ($h_n = 1$ or $h_n = 0$) there is no reduction made (pixels values are not modified). Their method employs the location map (LM) to record modifications performed in each pixel. The LM plays a significant role while extracting data. Hence, the LM defined in (19) was given and as this method is reversible, the recovery of the original difference was carried out using (20).

$$LM = \begin{cases} 0 & \text{if } 2^{\lfloor log_2 h'_n \rfloor} = 2^{\lfloor log_2 h_n \rfloor} \text{ or } h'_n = h_n \\ 1 & \text{if } 2^{\lfloor log_2 h'_n \rfloor} \neq 2^{\lfloor log_2 h_n \rfloor} \end{cases} \quad (19)$$

$$z_n = \begin{cases} z'_n + 2^{\lfloor log_2 z'_n \rfloor - 1} & \text{if } LM = 0 \\ z'_n + 2^{\lfloor log_2 z'_n \rfloor} & \text{if } LM = 1 \end{cases} \quad (20)$$

Accordingly, their experimental results reveal that reducing the difference before concealing data preserves good visual quality of the stego image and embedding capacity as well.

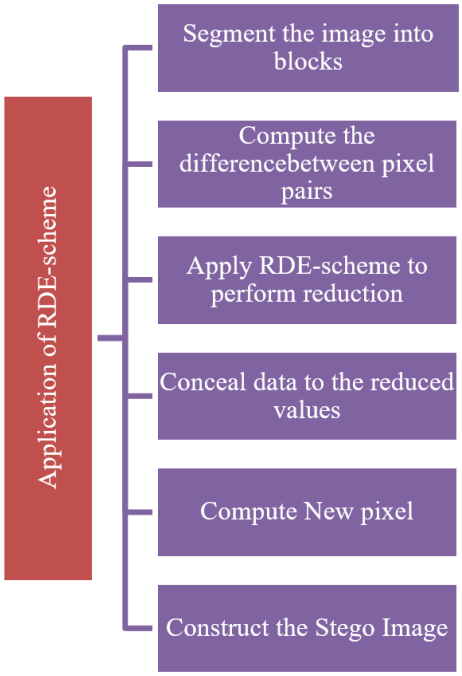

Fig. 6. Steps for applying the RDE-scheme

F. Improved Reduced Difference Expansion

Yi *et al.* [5] presented an improvement of Lu *et al.* 's work [21] which greatly enhanced the embedding capacity. Their proposed method is a multilayer data hiding which embeds data in different layers. In (21), the new improved reduced difference expansion (IRDE) scheme developed by Yi et al is given, where $n = \lfloor log_2 |h_n| \rfloor$ and h_n denotes the difference to be reduced. When values of the difference obtained after reduction are in the defined range ($3 \times 2^{n-1} \leq z_n \leq 4 \times 2^{n-1} - 1$), the reduction process results into small values to be employed for concealing data.

$$h'_n = \begin{cases} z - 2^{\lfloor log_2 h_n \rfloor - 1} & \text{if } 2 \times 2^{n-1} \leq h_n \leq 3 \times 2^{n-1} - 1 \\ z - 2^{\lfloor log_2 h_n \rfloor} & \text{if } 3 \times 2^{n-1} \leq h_n \leq 4 \times 2^{n-1} - 1 \end{cases} \quad (21)$$

The extraction of the embedded data and restoration of the original cover image were performed based on the location map in (22) which was assigned during the

application of the improved RDE-scheme in (21) and values of the reduced difference were restored by utilizing (23).

$$LM = \begin{cases} 0 & \text{if } 2 \times 2^{n-1} \leq z_n \leq 3 \times 2^{n-1} - 1 \\ 1 & \text{if } 3 \times 2^{n-1} \leq z_n \leq 4 \times 2^{n-1} - 1 \end{cases} \quad (22)$$

$$z'_n = \begin{cases} z_n + 2^{\lfloor log_2 z_n \rfloor + 1} & \text{if } LM = 1 \\ z_n + 2^{\lfloor log_2 z_n \rfloor} & \text{if } LM = 0 \end{cases} \quad (23)$$

The highest peak signal-to-noise ratio (PSNR) value and the embedding capacity over Lu et al.'s method were achieved after concealing data in the first layer while for the last three layers Lu *et al*.'s method outperforms Yi et al.'s one in terms of the embedding capacity.

G. RDH Based on Modified Difference Expansion

The Reversible Data Hiding (RDH) method based on modified difference expansion was implemented by Khodaei and Faez [22]. Their method is a lossless block-based that uses similarity between neighboring pixels to ameliorate the performance. During the first stage data were concealed in the cover image and in the second stage the extraction of data and the original cover image recovery were carried out. These two steps are summarized as follows.

a) Embedding stage

The embedding stage was accomplished by first segmenting the cover image M into blocks of size $k \times k$ which are not overlapped. Thereafter the steps mentioned below were performed.

1. Determine the central pixel (k_c) in each generated block
2. Use the central pixel to calculate the difference between pixel pairs using (24). Note that pixels are denoted by k_i and h_i represents the i^{th} difference

$$h_i = k_i - k_c \quad (24)$$

3. Conceal bits (s) of the confidential data by modifying the difference h_i to get the expanded difference h'_i as in (25)

$$h'_i = (h_i + s) \times 2 \quad (25)$$

4. Apply (26) to compute the new pixel value (pixel having confidential data)

$$k'_i = \begin{cases} k_c - h'_i & \text{if } k_i < k_c \\ k_c + h'_i & \text{if } k_i \geq k_c \end{cases} \quad (26)$$

5. Build the stego image by replacing the new pixels into the original cover image. The output is the stego image M' having all hidden confidential data is ready to be shared over the network
6. End the embedding script

b) Extracting stage

Similar to the embedding process, to be able to extract data (s) and restore the original cover image (M), the block of the same size $(k \times k)$ are constructed from the stego image M' after that the extraction process continues by executing the steps mentioned mentioned in (27), (28), and (29).

1. Select the central pixel from each block
2. Access pixels in each block to compute the difference between them by applying (27)

$$h'_i = k'_i - k_c \quad (27)$$

3. Perform the extraction of the hidden bits (s) using (28)

$$s = h'_i \bmod 2 \quad (28)$$

4. Restore the original pixel values (k_i) using equation in (29)

$$k_i = \begin{cases} k_c - \left\lfloor \frac{h'_i}{2} \right\rfloor, & if\ k'_i < k_c \\ k_c + \left\lfloor \frac{h'_i}{2} \right\rfloor, & if\ k'_i \geq k_c \end{cases} \quad (29)$$

5. Reconstruct the original cover image by substituting stego pixels values for the recovered ones (k_i) pixels obtained in (29) The output is the same original cover image without any degradation
6. End the extraction script

Different block sizes $(2 \times 2,\ 3 \times 3,\ 4 \times 4,\ 5 \times 5)$ were used to evaluate the impact of increasing the block size on the embedding capacity and based on their experimental results the block of size 5 by 5 $\rightarrow (5 \times 5)$ achieves the highest embedding capacity over the other types of block size.

H. Difference Expansion for Medical Images

Large smooth areas are one of the characteristics of medical images. To exploit this advantage, Al-Qershi and Khoo [23] proposed a new difference expansion method that increases the payload capacity for medical images. Two regions, namely, smooth regions and non-smooth regions were considered in the cover image. The smooth algorithm was applied to hide high payload capacity while the original difference expansion algorithm was employed to conceal data in non-smooth regions. Note that their method has combined three information hiding schemes from Tian [3], Alattar [18] and Chiang et al.'s work [24]. The experimental results obtained after testing the proposed mothed using sixteen medical cover images show that high payload capacity was achieved.

I. PVM-based on Modulus Function

A pixel value modification data hiding scheme developed using modulus function was provided by Nagaraj et al. [7] in 2013. The embedding process was performed by splitting up three components, i.e., Red (R), Green (G) and Blue (B) of the colored image. Every pixel has 24 bits with 8 bits allocated to each component and confidential data were embedded in each color component. The modification of the pixel values was performed sequentially by first hiding data in the first component and to improve the quality of the stego image different criterions were defined to control the embedding process.

TABLE I: SUMMARY ON THE PERFORMANCE OF VARIOUS TECHNIQUES PRESENTED IN THIS SURVEY

Information Hiding approach	Type of the cover Image	Size of the Pixel Block	Payload capacity in bits or bit per pixel (bpp)	Invisibility (PSNR in decibels dB)
Tian [3]	Grayscale image	2 ×1	High	≥16.47
Alattar [18]	RGB image	2 ×2	High	≥24.73
Angreni and Ahmad [19]	Grayscale image	2 ×1	Medium	≥51.15
Lee et al. [20]	Grayscale image	2 ×2	High	≥30.86
Lou et al. [21]	Grayscale image	2 ×1	High	≥22.41
Yi et al. [5]	Grayscale image	2 ×1	High	≥35.17
Khodaei and Faez [22]	Grayscale image	2 × 2, 3 × 3 4 × 4, 5 × 5	High	≥33.09
Al-qershi and Khoo [23]	Grayscale image	4 ×4	High	≥39.02
Nagaraj et al. [7]	RGB image	-	Medium	≥39.06
Arham et al. [4]	Grayscale image	2 ×2	High	≥31.98
Kurniawan et al. [25]	RGB image	2 ×2	High	≥47.90

J. Multilayer DE for Medical Images

In 2017, a multilayer data hiding approach that is based on difference expansion of quad intending to increase the payload capacity and visual quality was developed in the work presented by Arham et al. [4]. This method is the combination of two approaches. The first one is the data hiding approach presented by Alattar [18] that conceals data into block of quads and the second one is the improved RDE that reduces difference values before hiding confidential data presented in the research carried out by Yi et al. [5]. The evaluation of the performance was accomplished using fourteen medical images and based on their experiment good results were achieved compared to the previous approaches. For Further information detailing the algorithm design refer to their work [4].

K. Modulo Fucntion Quad-DE

Taking the advantages of difference expansion approach and modulo function, in 2016 Kurniawan et al. [25] built a new RDH approach that uses both techniques. To prevent the new pixel value from being highly increased which may results in decreasing the PSNR value (the visual quality of the stego image), the modulus of the difference was first computed. After that those values were compared to their respective difference before embedding data. For example, if h_1 is the value obtained after computing the difference between two adjacent pixels p_1 and p_2 with $h_1 \rightarrow p_1 - p_2$, before embedding the data the modulo of h_1 is calculated as $k = h_1 \bmod n$ with k denoting the modulo value of h_1 and n representing the base number which can be in the set, $n \rightarrow \{2, 3, 4, 5, 6 \ldots.\}$. Now k value must be compared with h_1 to decide whether the value of the pixel has to be modified or kept intact. The experimental results and analysis proves that this method has increased the embedding capacity while also achieving a good visual of the stego image. Correspondingly, Table I presents a summary on the overall performance of the method presented in this survey.

V. CONCLUSION

Information hiding has become among the valuable and essential security techniques for securing communication through the internet while sharing multimedia confidential data. The main goal of information hiding method is to secure sensitive data by providing a covert communication, i.e., the data transmission and sharing are kept secret between the sender and the authorized receiver to ensure the user right, privacy, copyright, data confidentiality, and data integrity. There exists various information hiding in the literature developed to maintain and protect the private information. High payload capacity and high visual quality of the stego image are the most aspects of any information hiding methods which ensure its security level, imperceptibility and robustness. This paper presents a comprehensive survey on the existing reversible data hiding approaches developed based on difference expansion, reduced difference expansion and pixel value modification combined with fundamental concepts and their performance analysis. Factors such as how to select the best cover image suitable for concealing data, process to determine the best image format, and finally how to achieve a high embedding capacity while preserving the quality of the stego image are still among the current challenges to be investigated. We hope that that the work presented in this survey can greatly assist researchers in

the field of information hiding to easily figure out the future research direction.

REFERENCES

[1] C. Lin and N. Hsueh, "A lossless data hiding scheme based on three-pixel block differences," *Pattern Recognit*., vol. 41, pp. 1415–1425, 2008.

[2] X. Zeng, Z. Li, and L. Ping, "International journal of electronics and communications (AEÜ) reversible data hiding scheme using reference pixel and multi-layer embedding," *AEUE - Int. J. Electron. Comm*., vol. 66, no. 7, pp. 532–539, 2012.

[3] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Tech*., vol. 13, no. 8, pp. 890–896, 2003.

[4] A. Arham, H. A. Nugroho, and T. B. Adji, "Multiple layer data hiding scheme based on difference expansion of quad," *Signal Processing*, vol. 137, pp. 52–62, 2017.

[5] H. Yi, S. Wei, and H. Jianjun, "Improved reduced difference expansion based reversible data hiding scheme for digital images," in *Proc. 9th International Conference on Electronic Measurement & Instruments*, 2009, pp. 315–318.

[6] 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.

[7] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color image steganography based on pixel value modification method using modulus function," *IERI Procedia*, vol. 4, pp. 17–24, 2013.

[8] S. Agrawal and K. Manoj, "Reversible data hiding for medical images using integer-to-integer wavelet transform," in *Proc. IEEE Students' Conference on Electrical, Electronics and Computer Science Reversible*, 2016.

[9] F. Peng, X. Li, and B. Yang, "Adaptive reversible data hiding scheme based on integer transform," *Signal Processing*, vol. 92, no. 1, pp. 54–62, 2012.

[10] H. Chen, J. Ni, W. Hong, and T. Chen, "Signal processing : Image communication reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering," *Signal Process. Image Comm*., vol. 46, pp. 1–16, 2016.

[11] Z. Yin, A. Abel, X. Zhang, and B. Luo, "Reversible data hiding in encrypted image based on block histogram shifting," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2016, pp. 2129–2133.

[12] C. N. Lin, D. J. Buehrer, C. C. Chang, and T. C. Lu, "Using quad smoothness to efficiently control capacity-distortion of reversible data hiding," *J. Syst. Softw.*, vol. 83, no. 10, pp. 1805–1812, 2010.

[13] J. V. C. I. R, W. He, J. Cai, K. Zhou, and G. Xiong, "Efficient PVO-based reversible data hiding using multistage blocking and prediction accuracy matrix q," *J. Vis. Commun. Image Represent.*, vol. 46, pp. 58–69, 2017.

[14] S. Han, H. L. Jin, M. Fujiyoshi, and H. Kiya, "Lossless data hiding in the spatial domain for high quality images lossless data hiding in the spatial domain for high quality images," in *Proc. International Symposium on Intelligent Signal Processing and Communications (ISPACS)*, 2006.

[15] K. Wang, Z. Lu, and Y. Hu, "A high capacity lossless data hiding scheme for JPEG images," *J. Syst. Softw*., vol. 86, no. 7, pp. 1965–1975, 2013.

[16] C. D. Vleeschouwer, J. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Trans. Multimed.*, vol. 5, no. 1, pp. 97–105, 2003.

[17] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Comput. Sci. Rev.*, vol. 13–14, no. C, pp. 95–113, 2014.

[18] A. M. Alattar, "Reversible watermark using difference expansion of quads," in *Proc. IEEE Int. Conf. Acoust. Speech, Signal Process*, 2004, no. 1, pp. 377–380.

[19] D. S. Angreni and T. Ahmad, "Enhancing DE-based data hiding method by controlling the expansion," in *Proc. International Conference on Cyber and IT Service Management*, 2016.

[20] C. Lee, H. Wu, C. Tsai, and Y. Chu, "Adaptive lossless steganographic scheme with centralized difference expansion," *Pattern Recognit*., vol. 41, pp. 2097–2106, 2008.

[21] D. C. Lou, M. C. Hu, and J. L. Liu, "Multiple layer data hiding scheme for medical images," *Comput. Stand. Interfaces*, vol. 31, no. 2, pp. 329–335, 2009.

[22] M. Khodaei and K. Faez, "Reversible data hiding by using modified difference expansion," in *Proc. 2nd International Conference on Signal Processing Systems*, 2010, no. 5, pp. 31–34.

[23] O. M. Al-qershi and B. E. Khoo, "High capacity data hiding schemes for medical images based on difference expansion," *J. Syst. Softw*., vol. 84, no. 1, pp. 105–112, 2011.

[24] K. H. Chiang, K. C. Chang-Chien, R. F. Chang, and H. Y. Yen, "Tamper detection and restoring system for medical images using wavelet-based reversible data embedding," *J. Digit. Imaging*, vol. 21, no. 1, pp. 77–90, 2008.

[25] 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 *Proc. International Conference on Advanced Computer Science and Information Systems*, 2016, pp. 433–437.

[26] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.