International Journal of Innovative
Computing, Information and Control
Volume **15**, Number **2**, April **2019**

ICIC International ©2019 ISSN 1349-4198
pp. **667–680**

HIGH QUALITY PVM BASED REVERSIBLE DATA HIDING METHOD FOR DIGITAL IMAGES

Pascal Maniriho and Tohari Ahmad

Department of Informatics
Institut Teknologi Sepuluh Nopember
Kampus ITS Surabaya, Jawa Timur 60111, Indonesia
tohari@if.its.ac.id

Received May 2018; revised September 2018

Abstract. *In recent years, transmitting and sharing multimedia data across the Internet have raised up many data security issues such as copyright and contents protection due to the communication channel (network) which is often insecure. Therein, the need for new data hiding security mechanisms like steganography has become a necessity. Steganography is the art and science of veiling the existence of the private message while keeping the communication invisible. To exploit this feature, a new reversible data hiding method based on pixel value modification (PVM) that allows secret data to be veiled into the carrier image is introduced in this paper. The proposed method employs the logarithmic predictor and the reference pixel to control the embedding process while the key indicator is used to record the position and the operations performed on each pixel. The embedded confidential data and the original carrier image can be reconstructed without any degradation. Besides, the experimental results, analysis and comparisons demonstrate that the quality of the stego image is better than those of existing methods.*
Keywords: Data hiding, Information security, Data protection, Pixel value modification

1. **Introduction.** Securing multimedia data has become a necessity due to the introduction of new technologies, along with massive growth of online communication platforms and network policy violations in recent years. Most of the online applications require various security techniques to secure data being shared across them via the open public network (Internet). Steganography is one of possible security techniques that is employed. The main goal of steganography is to veil secret data into the carrier media such as text, audio, image and video and to convey them to the destination while keeping the communication invisible. Various types of steganographic techniques which are available in the literature can be viewed in Figure 1. An image or audio is popular for veiling the secret data; it is called image or audio steganography and its output is the stego image or audio holding the embedded data [1, 2]. Correspondingly, each digital image possesses areas called regions which are not greatly changed by some designated image processing operations such as contrast enhancement, image cropping, or alteration of pixel value. This characteristic makes them to be invariant to attacks while conveying multimedia data over a non-protected network [3].

The image steganography-based methods are mainly classified into spatial, compression and frequency domains. In addition, methods developed based on these domains can be reversible (the carrier media and concealed data can be recovered) or irreversible (only the concealed data can be recovered). The methods in the spatial domain conceal confidential data into the carrier media by immediately modifying the value of the pixel. Nevertheless,

DOI: 10.24507/ijicic.15.02.667

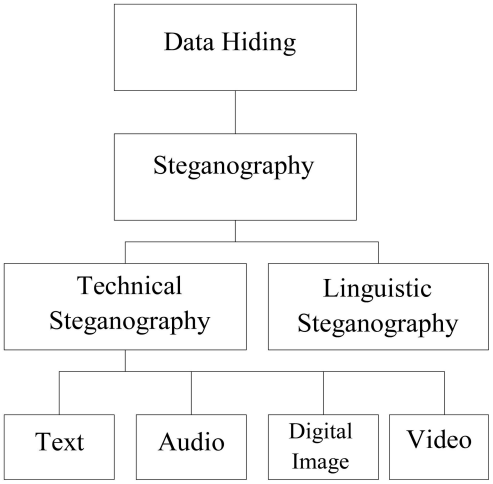

FIGURE 1. Security techniques in steganography

in the frequency domain, the secret is embedded into the frequency coefficients obtained after transforming the carrier media from spatial to frequency domain. Images having series of compressed codes are adopted in the compression domain as the best carrier media, i.e., the data are concealed by altering the compressed codes. Pixel value differencing (PVD) [4], the least significant bits (LSB) [5] and difference expansion (DE) [3, 6] are some famous spatial domain methods which have gained popularity in image-based steganography. On the other hand, discrete wavelet transform (DWT) [7, 8] and discrete cosine transform (DCT) [9, 10] are the most popular techniques in the frequency domain. The approach in [9] has the ability to embed a large size of secret data into the discrete cosine transform coefficients of the carrier image. Patient records can be secured using the electrocardiogram (ECG) steganography during their transmission, i.e., data can be concealed into an abdominal ECG signal using singular value decomposition (SVD) and discrete wavelet transform in medical image-based steganography [11].

Furthermore, methods employing the compression domain exist as well [12, 13]. To keep the quality of the compressed image, the compression was performed using the discrete cosine transform and discrete wavelet transform (DWT) [14]. Whether the method is implemented in any of the aforementioned domains, remarkable modifications in the carrier image are always avoided since they may raise up high dissimilarities between the original carrier media and the corresponding stego image which can arouse the attackers interests. That is, to keep the communication invisible such drastic changes must be prevented from the stego image so as to mask the attacker intending to violate user right, privacy and copyright protection.

More importantly, the need for returning the same carrier image into its original form after the recovery of the secret data has gained attention in some of the data hiding application domains such as law enforcement, military documents, medical imaging systems, limited bandwidth communication systems, image transcoding and multimedia archive management, i.e., in such situations the reversibility of the data hiding approach becomes a requirement [15]. Consequently, a new reversible image steganographic method based on pixel value modification (PVM) is implemented in this paper. Specifically, we introduce two parameters, namely, logarithmic predictor, reference pixel which are computed to control the embedding process in order to maintain the similarity between the original carrier and its corresponding stego image after embedding the secret data. Besides, the third parameter, is the key indicator which is used to record the status of each pixel

(the modifications made in each pixel). The values assigned to the key indicator variable are further used for recovering the embedded data and the original carrier image. The comparison on the experiment results shows that the proposed method maintains a high quality of the stego image over the previous schemes.

This paper is structured as follows. The previous work is described in Section 2 while the proposed method is provided in Section 3 and Section 4 elaborates the evaluations metrics. The experimental results and analysis are presented in Section 5. Finally, the conclusion is given in Section 6.

2. **Related Work on Image-Based Data Hiding.** Various existing reversible image steganographic methods including PVM are briefly introduced in this section. The least significant bit (LSB) insertion is among the easiest image steganographic techniques [16]. The insertion is made by replacing one or more LSB bits with the secret bits. However, attention needs to be taken since the more substituted LSBs are, the more the dissimilarity between images increases. Moreover, using a 24-bit red-green-blue (RGB) carrier image minimizes the degree of dissimilarity between the original carrier and the stego images. Such dissimilarity minimization makes the changes performed in the cover image to be unnoticeable to human eye. In other words, perceiving some visual modifications should be infeasible for the human eye. To demonstrate how the LSB bits in the carrier image are substituted for the secret data, let us take the example of four neighboring pixels from RGB carrier image whose binary encoding representation is presented in Table 1.

TABLE 1. R, G, B image pixels encoded in binary

1st pixel	2nd pixel	3rd pixel	4th pixel
11010101	10101101	11001011	10010111
11010110	11001111	11101010	10010110
10011111	01010000	11001011	11011111

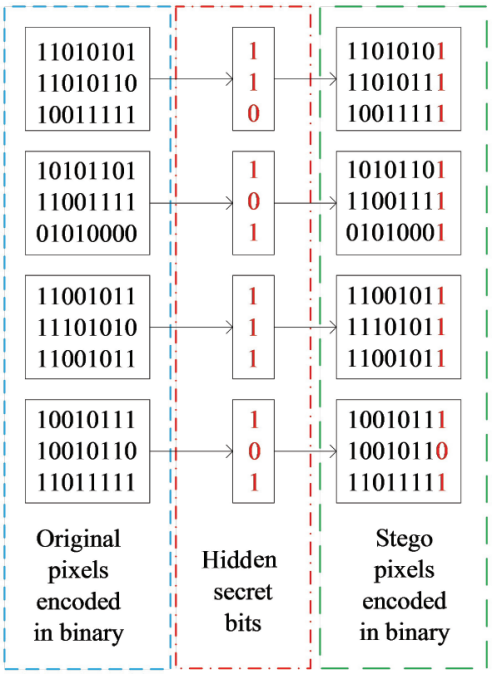

FIGURE 2. Secret bits insertion in the least significant bit

Assuming that 12 bits (110101111101) of the secret data have to be embedded in the four pixels presented in Table 1, the LSB substitution can be depicted in Figure 2 where the group of bits in the middle indicates the hidden secret bits. The extraction of the hidden bits can be accomplished by taking the LSBs of the encoded binary stego images. The LSB substitution was applied to embedding secret data in the contour regions of the carrier image [7]. To improve the security of image steganography, an approach that randomizes the embedding process using two secret keys was presented by Dagar [17]. Besides, their approach hides data into the three channels of the RGB image. The difference expansion and the modulus functions were used to build a scheme that relatively achieves better embedding capacity and quality of the stego image [18]. Details on image steganography coupled with its applications were presented in [19]. Blocks of quad-based DE (QDE) [20] and reduced DE (RDE)-based schemes [21] were joined to develop a high payload multilayer data hiding approach that was built in [22]. The adaptive information hiding scheme to conceal data in a high dynamic range carrier images encoded in OpenEXR format was presented by Lin et al. [23]. Furthermore, in order to hold more confidential bits, an adaptive algorithm for embedding secret data in the pixels with low luminance was also introduced in their work. The performance analysis on data hiding models based on pixel value differencing was elaborated by Lee et al. [24]. The additive modulo and mean value were employed to design a new reversible data hiding model for transformed images [25]. The encryption was accomplished using additive modulo while the mean value was used to insert the secret data into the encrypted image. Difference expansion and modulus functions were utilized to build the information hiding scheme introduced by Maniriho and Ahmad [26]. In He et al.'s work [27] the embedding was performed by grouping pixel values.

The distortion of the stego image can be decreased using Weng et al.'s reversible data hiding (RDH) method which was implemented using the "block-partition and adaptive pixel modification" techniques [28]. Original pixels of the cover image were classified as complex regions and smooth regions so as to allow high embedding capacity to be achieved while maintaining the quality of the stego image [29]. Chen et al.'s RDH model has increased the payload capacity and peak signal to noise ratio (PSNR) value by employing the histogram shifting combined with pixel value ordering [30]. The high redundancy encountered in image was exploited by He et al. who proposed a multistage blocking approach [31]. The prediction accuracy matrix was applied to improving the efficiency and the performance of their proposed algorithm. The contrast enhancement was applied to the carrier image's regions of interest without causing the additional deformation in the data hiding structure introduced by Gao et al. [32] that conceals secret message in medical images. Genetic algorithm was applied to constructing the data hiding model that hides data in the right places of the image [33]. To enable the block redundancy mining different sizes of pixel blocks were adopted in [34]. Another fully reversible algorithm based on binary-blocking for encrypted images was presented in [35].

Motivated by several smooth regions encountered in medical image, the payload capacity was increased in Al-qershi and Khoo's work [36]. Their method segments the medical cover image into two main regions namely, smooth and non-smooth regions. Smooth regions were used to accommodate more secret bits while few bits were veiled into non-smooth regions after applying the difference expansion technique. The visual quality and payload capacity were greatly enhanced in the approach that hides secret data into non-overlapped pixel block of the carrier image [37]. The secret data were embedded by utilizing histogram shifting generated using the difference values computed between neighboring pixels [38]. Confidential data were concealed in medical and non-medical digital images using the RDE-based approach developed in [39].

Khodaei and Faez [40] have used the difference expansion to implement a lossless block-based RDH method. Moreover, their method employs the similarity between nearby pixels (pixel which are neighbors) to enhance the performance. The embedding was performed through the following procedures. The carrier image was primarily partitioned into non-overlapped blocks having the size of $m \times n$ after that the central pixel (c_P) was determined in each block. The difference (v_i) between pixels in each block was computed using the expression in (1); while (2) was employed to embed the secret data (s). Note that p_i indicates the original pixel and v_i' is the extended difference after adding the secret bit to v_i. The stego pixel (p_i') was calculated using (3) thereafter all pixels holding data were used to construct the stego image.

$$v_i = p_i - c_p. \tag{1}$$

$$v_i' = (v_i + s) \times 2. \tag{2}$$

$$p_i' = \begin{cases} c_p - v_i', & \text{if } p_i < c_p \\ c_p + v_i', & \text{if } p_i \geq c_p \end{cases} \tag{3}$$

The extraction was performed by selecting the central pixel from each block which was further utilized to compute the difference between pixels as it is shown in (4). Besides, (5) is the expression for recovering the secret data whereas (6) is for restoring the original pixel values.

$$v_i'' = p_i' - c_{p'}. \tag{4}$$

$$S = v_i'' \bmod 2. \tag{5}$$

$$p_i = \begin{cases} c_p' - \left\lfloor \dfrac{v_i'}{2} \right\rfloor, & \text{if } p_i' < c_p \\ c_p' + \left\lfloor \dfrac{v_i'}{2} \right\rfloor, & \text{if } p_i' \geq c_p \end{cases} \tag{6}$$

The performance of this method was evaluated using different sizes of pixel block such as (2×2, 3×3, 4×4, and 5×5) and based on the experimental results, the highest embedding capacity was achieved with (5×5) block. PVM-based data hiding methods have proved the ability to preserve a relatively high similarity between the carrier and its respective stego image. The examples are the PVM-based methods that disguise data into the components of the RGB colored image which were presented in [41, 42].

3. **The Proposed Method.** The goal of the pixel value modification techniques is to prevent pixel values from being greatly modified in order to respond to the trade-off between the quality of the stego image and the embedding capacity. Considering this concept, a new reversible PVM-based image steganographic method is presented in this work. The proposed method is highly based on three parametric techniques, namely, logarithmic predictor, reference pixel and key indicator. At the early stage we assume that the carrier (cover) media is an 8-bit grayscale image Y having pixels $Y(i,j) \in [0, 255]$, i.e., $0 < Y(i,j) < 255$ where (i,j) represents the pixel located at the n^{th} position in Y. The reference pixel denoted by *Ref_pix* is obtained by computing the cover image pixels' average thereafter the logarithm predictor (Lp) is applied to each pixel value and the obtained reference pixel to determining whether the pixel has to be modified or kept intact. Besides, the key indicator (K_i) is utilized to record the position and the operations performed on each pixel $Y(i,j)$. Accordingly, the proposed method can be mainly split up into two parts specifically: the embedding part (which gives procedures for embedding secret data) and extraction part (which discusses procedures for extracting the embedded secret data and the recovery of the original carrier image). Furthermore, the key indicator

is used in the extraction to recover the secret data and to reconstruct the original cover image as the proposed method is completely reversible.

3.1. **Procedures for embedding the secret data.** The details on the embedding procedures are presented as follows. Let Y be an 8-bit grayscale cover image of size $(H \times T)$ whose pixels are denoted by $Y(i,j)$. Moreover, S denotes the bits of the secret data to be held by the carrier image (Y). Hence, having Y and S the data embedding can be accomplished by performing all steps provided below.

- Read (load) the 8-bit grayscale cover image $\rightarrow Y$
- Load the text file (file with *.txt extension) that contains the secret data to be embedded $\rightarrow S$
- Generate the reference pixel $\rightarrow$ *Ref_pix* value by computing the cover image pixels' average using (7).

$$Ref\_pix = \frac{1}{H \times T} \sum_{i=1}^{H} \sum_{j=1}^{T} Y(i,j). \tag{7}$$

- Apply the expressions below to calculating the logarithmic predictor (Lp) for each pixel value using (8) and the other one denoted by *Lp_Ref_pix* (see (9)) for the reference pixel value (Ref_pix) obtained in (7).

$$Lp(i,j) = \lfloor \log_2 Y(i,j) \rfloor. \tag{8}$$

$$Lp\_Ref\_pix = \lfloor \log_2 Ref\_pix \rfloor. \tag{9}$$

- Compare the results obtained using Equation (8) and the one from (9) using the expression in (10), to find the corresponding condition, whether it is true or false.

$$\text{embeddable} = \begin{cases} \text{true}, & \text{if } Lp \leq Lp\_Ref\_pix \\ \text{false}, & \text{if } Lp > Lp\_Ref\_pix \end{cases} \tag{10}$$

- If $Lp \leq Lp\_Ref\_pix$, the corresponding pixel value $Y(i,j)$ is embeddable, i.e., it is employed to hide the secret data S whose value can be either zero or one. More importantly, in case the condition in (10) evaluates to true, embed data and assign the value to the key indicator variable (K_i) according to the following criteria. If the embeddable pixel value is even $(Y(i,j) \bmod 2 = 0)$ and the secret bit is zero $(S = 0)$, then (11) is used to embed data and the K_i variable takes the value of $1 \rightarrow (K_i = 1)$. In addition, if the embeddable pixel is even and the secret bit is 1 $(S = 1)$, the embedding is also achieved using (11); however, 2 is assigned to K_i, $\rightarrow (K_i = 2)$. The third case is encountered when the embeddable pixel $Y(i,j)$ is odd $(Y(i,j) \bmod 2 = 1)$ and the secret bit is zero $(S = 0)$. In this case the embedding is carried out by utilizing (12) and K_i variable takes the value of $3 \rightarrow (K_i = 3)$ whereas if $(Y(i,j) \bmod 2 = 1)$ and $S = 1$, then the data are also hidden using (12) and 4 is assigned to K_i variable, $\rightarrow (K_i = 4)$.

$$Y'(i,j) = Y(i,j) + S. \tag{11}$$

$$Y'(i,j) = (Y(i,j) - 1) + S. \tag{12}$$

- If the condition in (10) is not met (false), the pixel value $Y(i,j)$ is kept unaltered (see (13)) and 5 is assigned to K_i variable $\rightarrow (K_i = 5)$. That is, there is no secret bit embedded into the pixel.

$$Y'(i,j) = Y(i,j). \tag{13}$$

- Considering the key indicators (values assigned to the K_i variable), the key values required to record changes are recorded as $K_i \in \{1, 2, 3, 4, 5\}$. Note that the defined key indicator values are used in the extraction while restoring the secret data and the value of the original pixel.
- Construct the stego image Y' by merging all stego pixels $Y'(i, j)$.
- Terminate the embedding script.

Having an 8-bit grayscale carrier image given in Figure 3 and the secret data S (0110), the embedding steps mentioned above, can be applied as follows. We first compute the reference pixel value which is obtained using (7) where the operation can be seen in (14). Note that the value of $m = H \times T$ is $20 \rightarrow (m = 20)$ and the sum of the pixel is 2463.

$$Ref\_pix = \left\lfloor \frac{2463}{20} \right\rfloor = 123. \tag{14}$$

50	67	200	99	145
130	187	100	111	120
125	123	55	202	83
198	178	88	35	167

FIGURE 3. An example of 8-bit grayscale carrier image, in which the box with dash line represents the pixels being processed

Let us check if the first pixel $P_1 = 50$ is suitable for embedding the secret data. As it was previously mentioned, the logarithmic predictor is used to determine the status of each pixel of the original carrier image. Therein, let us apply (8), (9) and (10) whose computations are given in (15), (16), and (17), respectively.

$$Lp = \lfloor \log_2(50) \rfloor = 5. \tag{15}$$

$$Lp\_Ref\_pix = \lfloor \log_2(123) \rfloor = 6. \tag{16}$$

$$Lp \leq Lp\_Ref\_pix \rightarrow 5 \leq 6. \tag{17}$$

From (17), it could be seen that the predicted value for the pixel in (15) is less than the one predicted for the reference pixel in (16), which exactly implies that the pixel is embeddable. The data is embedded by applying (11) and the operation can be seen in (18) and (19). For the first case, $S = 0$ is hidden and since $50 \bmod 2 = 0$, 1 is assigned to $K_i \rightarrow (K_i = 1)$ whereas for the second case $K_i = 2$ as $S = 1$.

$$P_1' = 50 + 0 = 50, \rightarrow S = 0 \text{ and } K_i = 1. \tag{18}$$

$$P_1' = 50 + 1 = 51, \rightarrow S = 1 \text{ and } K_i = 2. \tag{19}$$

Now the original pixel $P_1 = 50$ leads to $P_1' = 50$ if the hidden bit is 0 and $P_1' = 51$ if the hidden bit is 1. The second example examines the case where the pixel value P_2 which is taken from the carrier image in Figure 3 is odd, i.e., $P_2 = 67$ where $67 \bmod 2 = 1$. As it was performed while embedding the secret bits in the first pixel (P_1), the same steps in (15), (16), and (17) are considered in this second scenario and the operations are given in (20), (21) and (22). Besides, (12) is used for embedding data where the computations can be found in (25) and (26). That is, 1 is first subtracted from the value of the pixel since it is odd and (23) or (24) is applied if the secret bit is $(S = 0)$ or $(S = 1)$, respectively. This allows the same secret bits and pixel value to be restored during the extraction.

$$Lp = \lfloor \log_2(67) \rfloor = 6. \tag{20}$$

$$Lp\_Ref\_pix = \lfloor \log_2(123) \rfloor = 6. \tag{21}$$

$$Lp \leq Lp\_Ref\_pix \rightarrow 6 = 6. \tag{22}$$

Since $Lp \leq Lp\_Ref\_pix$, P_2 is embeddable and P_2' denotes the stego pixel.

$$P_2' = (67 - 1) + 0 = 66, \rightarrow S = 0 \text{ and } K_i = 3. \tag{23}$$

$$P_2' = (67 - 1) + 1 = 67, \rightarrow S = 1 \text{ and } K_i = 4. \tag{24}$$

The original pixel $P_2 = 67$ becomes $P_2' = 66$ if the hidden bit is 0 and $P_2' = 67$ if the hidden bit is 1. The stego image obtained after hiding data in both pixels (P_1' and P_2') can be seen in Figure 4; while the embedded bits can simply be recorded as $S = (0101)$ where the same data have to be recovered after the extraction. The illustration of the extraction procedures is depicted in Figure 5.

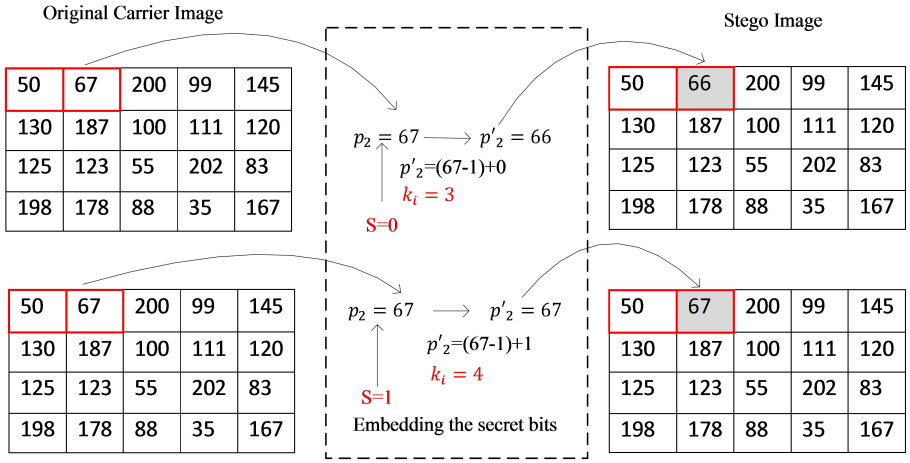

FIGURE 4. An 8-bit grayscale carrier image and its respective stego image after embedding secret bits in the first pixel (p_1) and the second pixel (p_2)

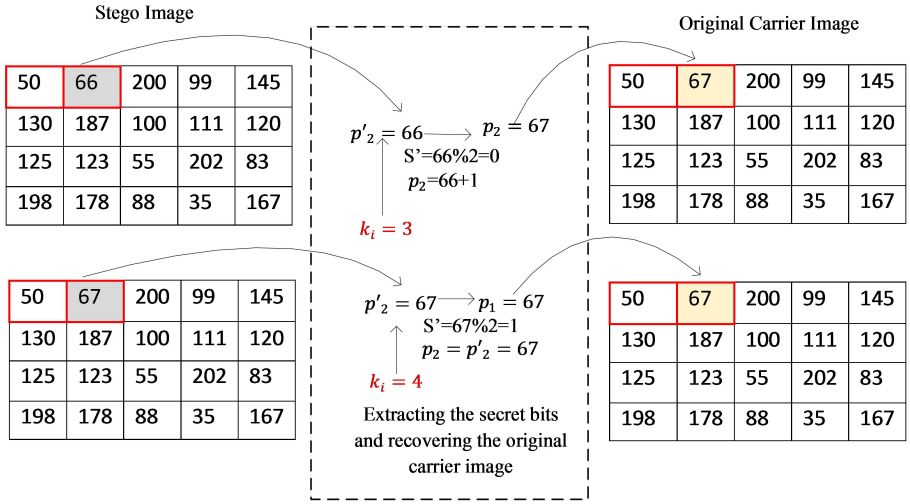

FIGURE 5. An 8-bit stego image and its respective original carrier image after extracting the secret bits and recovering the original first pixel (p_1) and the second pixel (p_2)

3.2. **Procedures for extracting the embedded secret data.** Extracting the embedded secret data and the reconstruction of the original carrier image are achieved by utilizing the key indicator values which were recorded during the embedding. In this way, the extraction is accomplished through these procedures. First, the stego image Y' and the variable (array) storing the key indicator are taken as inputs and after being fed to the extraction algorithm the operations below are executed based on the defined extraction criteria.

- If the key indicator value ($K_i = 1$), then the secret bits (S') are retrieved using Equation (25) and the original pixel is computed as shown in (26).

$$S' = Y'(i,j) \bmod 2, \quad \text{if } (K_i = 1). \tag{25}$$

$$Y(i,j) = Y'(i,j), \quad \text{if } (K_i = 1). \tag{26}$$

- If the key indicator value ($K_i = 2$), the secret bits are also recovered using (25) as performed in (27), and (28) is employed to get the original pixel value.

$$S' = Y'(i,j) \bmod 2, \quad \text{if } (K_i = 2). \tag{27}$$

$$Y(i,j) = (Y'(i,j) - 1), \quad \text{if } (K_i = 2). \tag{28}$$

- If ($K_i = 3$) the secret data is retrieved using (29) and (30) is employed to get the original pixel value.

$$S' = Y'(i,j) \bmod 2, \quad \text{if } (K_i = 3). \tag{29}$$

$$Y(i,j) = (Y'(i,j) + 1), \quad \text{if } (K_i = 3). \tag{30}$$

- If ($K_i = 4$) the secret data is retrieved using (31) and (32) is employed to get the pixel value.

$$S' = Y'(i,j) \bmod 2, \quad \text{if } (K_i = 4). \tag{31}$$

$$Y(i,j) = Y'(i,j), \quad \text{if } (K_i = 4). \tag{32}$$

Correspondingly, given the stego pixels ($P'_1 = 50$ or $P'_1 = 51$) and ($P'_2 = 66$ or $P'_2 = 67$) which can be found in the stego images depicted in Figure 4, the extraction process is demonstrated as follows.

1) Performing the extraction for $P'_1 = 50$
   For $P'_1 = 50$ with $K_i = 1$, the hidden data S' are extracted using (25) and the original carrier image pixels value is recovered using (26) as it is shown in (33).

$$S' = (50 \bmod 2) = 0; \quad \text{and } P_1 = P'_1 = 50. \tag{33}$$

2) Performing the extraction for $P'_1 = 51$
   For $P'_1 = 51$, and $K_i = 2$, also extract the hidden data S' using (27) and recover the original pixel value using (28) whose computations are given in (34).

$$S' = (51 \bmod 2) = 1; \quad \text{and } P_1 = 51 - 1 = 50. \tag{34}$$

3) Performing the extraction for $P'_2 = 66$
   For $P'_2 = 66$, and $K_i = 3$, extract the embedded data S' using (29) and restore the original pixel using (30) whose computations are performed in (35).

$$S' = (66 \bmod 2) = 0; \quad \text{and } P_1 = 66 + 1 = 67. \tag{35}$$

4) Performing the extraction for $P'_2 = 67$
   For $P'_2 = 67$, and $K_i = 4$, extract the hidden data S' using (31) and recover the original pixel using (32) whose computations are given in (36).

$$S' = (67 \bmod 2) = 1; \quad \text{and } P_1 = P'_1 = 67. \tag{36}$$

The recovered secret data $S' = (0101)$ and the original pixels value ($P_1 = 50$ and $P_2 = 67$) prove the reversibility of the proposed image steganographic method. That is, they match and the message is said to be authentic as there is no distortion encountered in the recovered data. Moreover, in Figure 4 and Figure 5 the "%" is the modulo operator.

4. **Evaluation Metrics.** The embedding (payload) capacity which is often measured in bits, kilobits (kb) or bit per pixel (bpp) and the peak signal-to-noise ratio (PSNR) are the well-known evaluation metrics that are utilized to assess and compare the performance of data hiding (steganographic) methods. The mathematical representation (formula) for computing the PSNR is given in Equation (37) where the MSE stands for the mean squared error between the original carrier and the stego images whose computation is given in (38). As well as that, the PSNR is considered as the measure of the peak error.

$$PSNR = 10 \times \log \frac{(MAX)^2}{MSE}. \tag{37}$$

$$MSE = \frac{1}{H \times T} \sum_{i=1}^{H} \sum_{j=1}^{T} \left(Y_{ij} - Y'_{ij}\right)^2. \tag{38}$$

In (38) the original n^{th} pixel in the carrier image (Y) is represented by Y_{ij} while the one in the respective stego image (Y') which is produced after hiding secret data is represented by Y'_{ij}. Besides, in (38) H and T represent the dimensions of the image. If the MSE value is lower, it implies that the error is also low and as it could be seen in (37), this results in a high PSNR value which gives a high similarity between the corresponding images (carrier image and stego image). That is, the data hiding approach achieving a high PSNR is the best one since the embedding is accomplished without noticeable visual artifacts on the stego image.

5. **Experimental Results and Analysis.** This section presents the results from the experiment where the performance of the proposed method is compared with Jaiswal et al.'s method [43] and Ahmad et al.'s method [44] by considering the capacity of the payload, PSNR and the computational time (execution time). The embedding capacity which is the size of secret data to be concealed is recorded in bits while the PSNR is measured in decibels (dB) in order to evaluate the degree of likeness between the original carrier image and the stego image. High degree of likeness (low deformation) is achieved when the PSNR value is high. The value of PNSR which is considerable to assure high image likeness was presented in Tang et al.'s work [45] which states that whenever the PSNR > 30 dB, the quality of the stego image is preserved.

Generally, in image steganographic models, the secret data must be concealed in way that prevents the carrier image from being worsened, i.e., the image visual quality must be maintained so as to minimize the potential that may arouse human eyes suspicions [16]. The performance of the proposed algorithm is evaluated using 512×512 grayscale images available in [46]. Furthermore, the results from the experiment are provided in Table 2 which presents the comparison between Jaiswal et al.'s method [43] and the proposed method, and Table 3 which depicts the comparison between Ahmad et al.'s method [44] and the proposed method.

With regard to the embedding capacity, various sizes of the secret data are considered, i.e., the same size of secret data is used for each image to evaluate the performance. For example, the same size of the secret data (51449 bits) is concealed into the carrier image (Car) using the proposed method, and the ones in [43, 44]. The results in both Tables 2 and 3 prove that the degree of likeness (in the essence of PSNR value) between the carrier image and the corresponding stego image generated after embedding the secret

TABLE 2. Comparison between the proposed method and Jaiswal et al. [43] in terms of visual quality (in decibel) and execution time (in seconds)

Carrier image	Payload capacity (kb)		PSNR (dB)		Execution time (s)	
	Jaiswal et al. [43]	Proposed method	Jaiswal et al. [43]	Proposed method	Jaiswal et al. [43]	Proposed method
Car	51449	51449	48.5831	60.4311	52.920	25.412
Truck	58626	58626	48.6470	58.5036	53.450	25.955
Elaine	41902	41902	48.4957	59.1464	54.662	25.174
Tank	40539	40539	48.4825	61.2468	52.920	25.167
Stream	37524	37524	48.4561	62.0676	52.999	25.262
Boat	51240	51240	48.5804	58.2653	54.577	25.430

TABLE 3. Comparison between the proposed method and Ahmad et al. [44] in terms of visual quality (in decibel) and execution time (in seconds)

Carrier image	Payload capacity (kb)		PSNR (dB)		Execution time (s)	
	Ahmad et al. [44]	Proposed method	Ahmad et al. [44]	Proposed method	Ahmad et al. [44]	Proposed method
Car	51449	51449	40.022	60.4311	3.837	25.412
Truck	58626	58626	37.645	58.5036	3.692	25.955
Elaine	41902	41902	41.1209	59.1464	3.378	25.174
Tank	40539	40539	38.2702	61.2468	3.388	25.167
Stream	37524	37524	35.0193	62.0676	3.765	25.262
Boat	51240	51240	39.846	58.2653	3.544	25.430

data is higher than the one from Jaiswal et al.'s method [43] and Ahmad et al.'s method [44]. Thus, it can be understood that such PSNR increment prevents the changes made from being noticeable to human eye which results in a covert or invisible communication. It should be also noted that the chances for tampering, altering and intercepting the embedded secret data are highly minimized. The Stream (also called Stream-bridge) carrier image achieves a high PSNR value (62.0676 dB) after embedding (37524 bits) whereas Truck achieves a low PSNR value (58.5036 dB) after veiling (58626 bits) of the secret data. Besides, the results show that for those carrier images (e.g., Truck and Car) accommodating many bits, the PSNR value is quite low compared to the other images.

Nevertheless, the PSNR value (60.4311 dB) generated after veiling the secret data (51449 bits) in Car is nearly similar to the one from Stream (62.0676 dB) with the capacity of (37524 bits) which entails that the features of the carrier image such as edges, low frequency contents, correlations between pixels, and region complexity can also have an impact on the quality of the visual quality of the stego image. That is, images possessing high correlation and low frequency such as Car can hold more secret bits with a high visual quality (lower degradation) than those with a high frequency like Stream. Normally, with reference to the value of the PSNR generated after embedding data into the images, the stego images cannot be easily differentiated from the original ones.

In addition, the execution time of this algorithm is measured and the results show that it does also vary according to the characteristics of the carrier image. The highest execution time is 25.955 seconds which is spent while embedding the secret data (58626 bits) into the Truck image. The lowest execution time, i.e., 25.167 seconds, is taken during the embedding in the Tank image. Generally, taking consideration of the time taken while

concealing data into all carrier images whose results can be seen in Tables 2 and 3, too much time is taken with Jaiswal et al.'s method [43] (with the execution time average of 53.588 seconds) which can be deduced that the proposed method is much faster (with the execution time average of 25.40 seconds) than that of Jaiswal et al.'s method [43]. However, Ahmad et al.'s method [44] outdoes the proposed one in terms of execution time. That is, the proposed method is 21.80 seconds (execution time average) slower than Ahmad et al.'s method [44] (with the average of 3.600 seconds). Accordingly, it can be concluded that the new method which is implemented in this paper is able to protect and secure sensitive data while keeping the communication invisible.

6. **Conclusion.** A new reversible method based on pixel value modification techniques for securing secret data while keeping the communication invisible is proposed in this paper. Reversible data hiding methods for digital image have gained reputations due to their ability to retrieve the hidden secret data and rebuild the original carrier image. In order to achieve a good embedding capacity while preventing changes made in the carrier image from arousing the attacker's interests, in this method, pixels which are appropriate for concealing the secret data are first identified using the suggested parameters (logarithmic predictor and the reference pixel) and the values assigned to the key indicator variable are further used to extract the embedded secret data and to recover the original pixel to be used for reconstructing the carrier image which is identical to the original one.

Besides, the mathematical expressions and illustrations presented in both embedding and extraction algorithms guarantee the reversibility of the proposed algorithm. As it could be found in the experimental results, the visual quality (which is determined based on the PSNR value) is better than those of the previous methods. Consequently, good embedding capacity and execution time are also achieved as well.

In the future work, the proposed method can be combined with the dual image technique to evaluate the variation of the quality of the stego image with respect to the embedding capacity. Another possible improvement on the proposed method can be carried out by optimizing the key indicator. As the parameter to store the information of the embeddable pixels, the key indicator should be as small as possible but is able to hold much information. This proposed method can be further extended, by reducing the difference between pixels. It is likely that smaller difference generates better stego image. This reduction may be performed by constructing blocks comprising uniform pixels. Nevertheless, this construction may affect the embedding capacity because only certain blocks are embeddable. Therefore, an algorithm which can compensate this capacity shortcoming is required.

REFERENCES

[1] 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.

[2] T. Ahmad and T. P. Fiqar, Enhancing the performance of audio data hiding method by smoothing interpolated samples, *International Journal of Innovative Computing, Information and Control*, vol.14, no.3, pp.767-779, 2018.

[3] 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.

[4] Himakshi, R. K. Singh, H. K. Verma and C. K. Singh, Bi-directional pixel-value differencing approach for RGB color image, *The 6th International Conference on Contemporary Computing (IC3)*, pp.47-52, 2013.

[5] M. Kalita and T. Tuithung, A novel steganographic method using 8-neighboring PVD (8nPVD) and LSB substitution, *Int. Conf. Syst. Signals, Image Process.*, vol.2016, pp.6-10, 2016.

[6] J. Tian, Reversible data embedding using a difference expansion, *IEEE Trans. Circuits Syst. Video Technol.*, vol.13, no.8, pp.890-896, 2003.

[7] A. Kaur, R. Kaur and N. Kumar, Image steganography using discrete wavelet transformation and artificial bee colony optimization, *The 1st International Conference on Next Generation Computing Technologies (NGCT-2015)*, 2015.
[8] T. Narasimmalou and R. A. Joseph, Discrete wavelet transform based steganography for transmitting images, *Int. Conf. Adv. Eng. Sci. Manag. (ICAESM)*, vol.2012, pp.370-375, 2012.
[9] Y. Lin, High capacity reversible data hiding scheme based upon discrete cosine transformation, *J. Syst. Softw.*, vol.85, no.10, pp.2395-2404, 2012.
[10] S. Lahiri, P. Paul, S. Banerjee, S. Mitra, A. Mukhopadhyay and M. Gangopadhyaya, Image steganography on coloured images using edge based data hiding in DCT domain, *IEEE the 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2016.
[11] E. S. Jero, P. Ramu and S. Ramakrishnan, Steganography in arrhythmic electrocardiogram signal, *The 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp.1409-1412, 2015.
[12] Y. Qiu, H. He, Z. Qian, S. Li and X. Zhang, Lossless data hiding in JPEG bitstream using alternative embedding, *J. Vis. Commun. Image Represent.*, vol.52, pp.86-91, 2018.
[13] Z. Pan and L. Wang, Novel reversible data hiding scheme for two-stage VQ compressed images based on search-order coding, *J. Vis. Commun. Image Represent.*, vol.50, pp.186-198, 2018.
[14] P. Telagarapu, J. V. Naveen, L. A. Prasanthi and V. G. Santhi, Image compression using DCT and wavelet transformations, *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol.4, no.3, pp.61-74, 2011.
[15] Z. Qian and X. Zhang, Lossless data hiding in JPEG bitstream, *J. Syst. Softw.*, vol.85, no.2, pp.309-313, 2012.
[16] M. S. M. Karim, S. Md. Rahman and I. Md. Hossain, A new approach for LSB based image steganography using secret key, *Proc. of the 14th International Conference on Computer and Information Technology (ICCIT 2011)*, pp.286-291, 2011.
[17] S. Dagar, Highly randomized image steganography using secret keys, *IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, 2014.
[18] Y. Kurniawan, L. A. Rahmania, T. Ahmad, W. Wibisono and R. M. Ijtihadie, Hiding secret data by using Modulo function in quad difference expansion, *International Conference on Advanced Computer Science and Information Systems (ICACSIS 2016)*, pp.433-437, 2016.
[19] M. S. Subhedar and V. H. Mankar, Current status and key issues in image steganography: A survey, *Comput. Sci. Rev.*, vols.13-14, pp.95-113, 2014.
[20] A. M. Alattar, Reversible watermark using difference expansion of quads, *IEEE International Conference on Acoustics, Speech, and Signal Processing*, no.1, pp.377-380, 2004.
[21] Y. Hu, W. Song and J. Hou, Improved reduced difference expansion based reversible data hiding scheme for digital images, *The 9th International Conference on Electronic Measurement & Instruments*, pp.315-318, 2009.
[22] 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.
[23] Y. Lin, C. Wang, W. Chen, F. Lin and W. Lin, A novel data hiding algorithm for high dynamic range images, *IEEE Trans. Multimed.*, vol.19, no.1, pp.196-211, 2017.
[24] C. Lee, J.-J. Li, C.-C. Chang and Y.-H. Wu, A survey of reversible data hiding schemes based on pixel value ordering, *Nicograph International (NicoInt)*, pp.68-74, 2016.
[25] S. Agrawal and M. Kumar, Mean value based reversible data hiding in encrypted images, *Optik*, vol.130, pp.922-934, 2017.
[26] 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.
[27] W. He, J. Cai, G. Xiong and K. Zhou, Improved reversible data hiding using pixel-based pixel value grouping, *Optik*, vol.157, pp.68-78, 2018.
[28] S. Weng, Y. Liu, J. Pan and N. Cai, Reversible data hiding based on flexible block-partition and adaptive block-modification strategy, *J. Vis. Commun. Image Represent.*, vol.41, pp.185-199, 2016.
[29] T. Nguyen, C. Chang and W. Chang, High capacity reversible data hiding scheme for encrypted images, *Signal Process. Image Commun.*, vol.44, pp.84-91, 2016.
[30] H. Chen, J. Ni, W. Hong and T. Chen, Reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering, *Signal Process. Image Commun.*, vol.46, pp.1-16, 2016.

[31] 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.
[32] G. Gao, X. Wan, S. Yao, Z. Cui and C. Zhou, Reversible data hiding with contrast enhancement and tamper localization for medical images, *Information Sciences*, vol.386, pp.250-265, 2017.
[33] M. Nosrati, A. Hanani and R. Karimi, Steganography in image segments using genetic algorithm, *The 5th International Conference on Advanced Computing & Communication Technologies Steganography*, pp.102-107, 2015.
[34] W. He, Improved block redundancy mining based reversible data hiding using multi-sub-blocking, *Signal Process. Image Commun.*, vol.60, pp.199-210, 2018.
[35] S. Yi and Y. Zhou, Binary-block embedding for reversible data hiding in encrypted images, *Signal Processing*, vol.133, pp.40-51, 2017.
[36] 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.
[37] M. Hussain, A. W. A. Wahad, A. T. S. Ho, N. Javed and K.-J. Jung, A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement, *Signal Process. Image Commun.*, vol.50, pp.44-57, 2017.
[38] 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.
[39] 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.
[40] M. Khodaei and K. Faez, Reversible data hiding by using modified difference expansion, *The 2nd International Conference on Signal Processing Systems (ICSPS)*, no.5, pp.31-34, 2010.
[41] 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.
[42] A. Laffont, P. Maniriho, A. Ramsi, G. Guerteau and T. Ahmad, Enhanced pixel value modification based on modulus function for RGB image steganography, *Int. Conf. on Inform. & Comm. Tech. and System*, 2017.
[43] S. P. Jaiswal, O. Au, V. Jakhetiya, A. Y. Guo and A. K. Tiwari, Adaptive predictor structure based interpolation for reversible data hiding, *Proc. of International Workshop on Digital-forensics and Watermarking (IWDW)*, pp.276-288, 2014.
[44] T. Ahmad, M. Holil, W. Wibisono and I. R. Muslim, An improved Quad and RDE-based medical data hiding method, *IEEE International Conference on Computational Intelligence and Cybernetics*, pp.141-145, 2013.
[45] M. Tang, J. Hu and W. Song, A high capacity image steganography using multi-layer embedding, *Optik*, vol.125, no.15, pp.3972-3976, 2014.
[46] University of Southern California, *SIPI Image Database*, http://sipi.usc.edu/database/database.php?volume=misc, [Accessed: 22-Oct-2017].