Journal of Engineering Science and Technology
Vol. 16, No. 5 (2021) 4160 - 4180
© School of Engineering, Taylor's University

AN EFFICIENT METHOD OF DATA HIDING FOR DIGITAL COLOUR IMAGES BASED ON VARIANT EXPANSION AND MODULUS FUNCTION

MUHAMMAD ZULQARNAIN[1,5] *, MUHAMMAD GHULAM GHOUSE[1],
WAREESA SHARIF[2], GHULAM JILANIE[3], AMNA SHIFA[4]

[1]Faculty of Computer Science and Information
Technology, Universiti Tun Hussein Onn Malaysia,
86400, Parit Raja, Batu Pahat, Johor, Malaysia
[2]Faculty of Computing Science, The Islamia
University of Bahawalpur, Punjab, Pakistan
[3]Department of Computer Science, Comsats
University Islamabad, Lahore Campus, Pakistan
[4]Department of Computer Science and IT, The Islamia
University of Bahawalpur, Punjab, Pakistan
[5]Riphah College of Computing, Riphah International
University Faisalabad Campus, Pakistan
*Corresponding Author: zulqarnainmalik321@gmail.com

Abstract

Nowadays information security over unsecured communication channels has become one of the superior challenging issues in this highly digitalized world. These issues have led to the application of the cryptography technique as a mean for securing data by encrypting them. The purpose of steganographic techniques considers three main key issues: high embedding capacity, good visual quality and security. In this paper, we present a better information concealing approach based on variant expansion and modulus function. It presents an improved methodology of steganography which enhance the ability of the concealed secret data and provides the high security of the stego-colour image. The proposed method adaptively considers the suitable embedding direction for each colour scale according to the higher embedding capacity. However, the previous approach has only examined smooth areas of an image where the difference value is 0 or 1 while neglecting other values for data hiding. Due to this limitation, the result is a decrease in the embedding capacity for all images containing some straight ranges. Therefore, a developed new method that selects both positive and negative difference values to hide secret data. From our experimental results and discussion, we demonstrate that our developed method obtains a higher capacity with peak signal-to-noise ratio (PSNR) of 54.74 dB, 52.68 dB, 46.37 dB, 54.08 dB, and 53.21 dB, for the respective images. Furthermore, the proposed method is tested for its effectiveness on different types of standard colour images and results showed enhanced imperceptibility of the stego image compared to state-of-the-art data hiding methods based on encoding function while maintaining suitable image quality.

Keywords: Confidential data, Data hiding, Data protection, Steganography, Variant expansion.

1. Introduction

Steganography is the art of hiding data in some media, preferably the digital media. Although, steganography is a prehistoric skill, however, computation makes it a powerful tool today [1]. Steganography enables us to obscure a secret message from the outside work rather than concealing the contents of a message like cryptography, hence a more secluded technique than any other competitor manner of message hiding [2]. It changes to cover image to implant secret message to communicate in any standard format so that these changes are not detectable by foreign. All through history, individuals expected to speak with each other, and now a constantly expanding number of individuals are utilizing electronic intends to send their messages. These same individuals are likewise turning out to be more mindful of their entitlement to protection, and what numbers of governments are acquainting new laws with battle fear based oppression without pondering the privilege to the security of the normal [3]. Presently, simply scrambling messages is not adequate, and with more PC infections available for use and the coming of spyware being utilized to take individual data and archives from home PCs, it has turned out to be important to guarantee that a client's close to home records are secure from assault. Encoding singular records tackled this issue however in doing as such presented another: if it is scrambled it must be worth encoding [4].

Steganography is information hiding into some channel [5]. The channel may be audio, video, text, protocol, or an image. When information is embedded into some media/channel, the quality of source media is disturbed. In the case of an image, the image quality is also affected. There are some techniques available in the literature to hide data into images, each one with its pros and cons. Even, different image formats have different methods of information hiding into them [6, 7]. Different researchers are utilizing steganography techniques for some security purposes. There are two similar terms steganography and cryptography used in the way that they both protect important information [8]. Steganography involves hiding information while cryptography encrypts the information [9]. The well structure of the steganographic scheme has completed three basic sections as known, transmitter, communication channel and recipient. In this way, in the digital steganographic process, the secret information can be hidden in a suitable cover image. The output is the stego image that can be immediately transmitted throughout the unsecured common networking, the idea of illustration presented in Fig. 1. Furthermore, some steganographic techniques that conceal data have faced a high degree of repetition in digital images have been previously demonstrated in [10]. A technique which is concealing confidential data in pixels are chosen arbitrarily was performed in [11] and for the performance of post-processing were applied by hybrid fuzzy neural network for stego images. Cheddad et al. [12] applied an versatile technique to embedding the texts in areas of interest of the cover image. There are several researchers have proposed various approaches based on different modulus function-based strategy and principle of PVD methods. However, some PVD based methodologies suffers from two main issues; (i) fall of boundary problem and (ii) low hiding capacity [13].

In this research, we focused on secure image steganography technique based on modulus function and compared the results with other traditional techniques reported for the same purpose. The histogram-based analysis presents that the proposed approach is better than the traditional LSB methods. It causes minimum variations in the original colour tone, which are impossible for the human eye to perceive and in many even undetectable during steg-analysis.

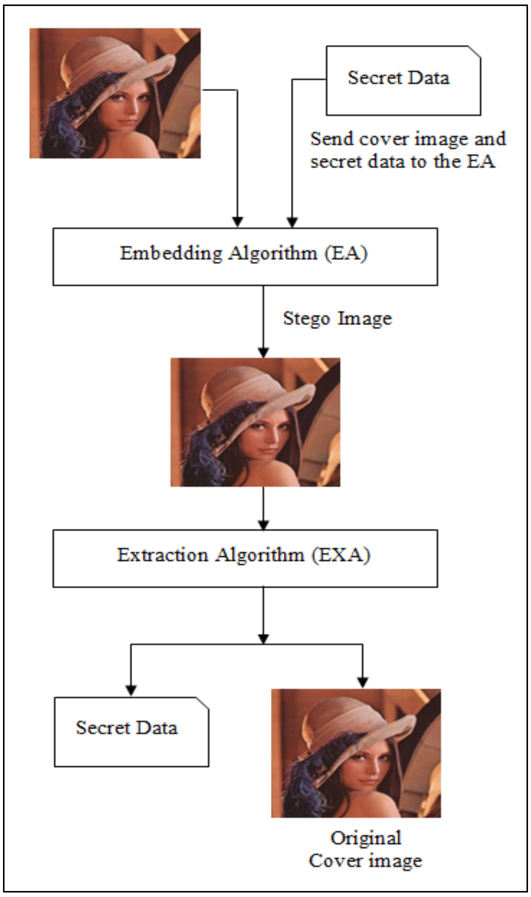


Fig. 1. Reversible digital image steganography.

In recent years, many information hiding methods have been developed which protect confidential data through concealing them into digital colour images. In this work, we proposed a steganography approach using the modulus function. This research improves embedding capacity, PSNR, and NPCR values using colour images based on the new variant expansion (VE) and modulus function-based data concealing strategy. Furthermore, during the extraction process, the modulus function is applied for the recovery of the concealed data. The key objective of our method is enhancing the embedding capacity whereas still keeping a sensible quality of the stego-image. By utilizing this procedure, we can store more information in the picture which is extremely valuable to send or get emit messages on a system. Furthermore, the proposed method divides each token of a message into three identical literals, and then the patterns of literals are matched with the individual pixels of the image from each red, green and blue portion. Where these three literals are matched, their position and length of a literal are packed to form a byte. Hence, a table namely LOG table is generated. This generated LOG table is then encrypted using Rijndael managed encryption algorithm.

The rest of this paper is organized as follows: Section 2 presents the recent trends in image steganography. Section 3 illustrates the proposed algorithm and modulus functions of steganography. Section 4 refers to the experimental results and discussion of the proposed method and the final conclusion of our work is described in Section 5.

2. Recent Trends in Image Steganography

In recent years, for secret communication, many researchers have been successfully used to incorporate different steganography approaches to conceal the data into the digital cover image [14-17], and achieved better results. Most of the researchers have applied soft computing tools which changed to be an immense jump in the history of steganography. Some of the research is referring to PVD-based methodologies which one of the most effective approaches to conceal confidential data into the spatial area. Such of these intelligent algorithms have allowed emerging secure secret information which achieved better performance in the term of PSNR and histogram. In this section, we briefly discuss some of the most effective PVD-based approaches in the fields of steganography. This PVD-based method minimizes the visibility of the concealing effect that was initially introduced by Wu and Tsai [18]. Similarly, Wang et al. [19] proposed a previous PVD method and applied modulus functions for decrease the perceptibility in the term of data concealing effect while improved the PSNR as compared original PVD approach. Based on the observation, this method obtained low embedding capacity in the concealed confidential data, while achieved a better quality of stego-image. For the grey images, Chang et al. [20] was introduced Tri-way Pixel Value Differencing (TPVD) algorithm. They utilized three-dimension variances ("horizontal, vertical and diagonal") are selected to eliminate the capacity constraint from the original PVD method and for embedding steps only use one direction. In steganography, more widely used algorithms in the spatial domain such as least significant bit (LSB) [21], histogram shifting [22], difference expansion [23], and integer transform [24]. These methods are mostly used when all values of image pixel or direct modification of precise are required. Furthermore, they obtain good embedding capacity but sometimes they are given the low stego-image quality. Variance expansion enables the secret information to be hidden by extending the modification values computed among pixels. Moreover, in recent, Sahu and Swain [25] was introduced an advance dual-layered based RIH approach using modified Least Significant Bit (LSB), in which enhanced the embedding capability using dual-layered based embedding strategy and curtail the distortion caused to the stego-image to enhance its quality after capturing the secret information and obtained better reversibility.

Similarly, Arham et al. [26] was introduced a reversible data hiding approach that conceals secret information in medical images while retaining both payload capacity and quality of the stego-image. Sahu and Swain [27] presented an advanced image steganography approach based on the principle of pixel overlapping to enhance the embedding capacity and PSNR, in which they have used two variants techniques such as overlapped pixel value differencing with modulus function (OPVDMF) and overlapped pixel value differencing (OPVD). Furthermore, EI-Emam and Al-Zubaidy [28] was referred a secure neural network based learning method with an additional layer that supports improving data security and protects against visual attacks. In [29] Mandal and Das were proposed

PVD scheme for colour image steganography in which addressed the issue of overflow in the pixel values of image. On the other hand, they also used PVD method for grey images in order to obtain higher level of security. Similarly, another method of intra colour PVD by combining with modulus function was suggested by Shen et al. [30]. Therefore, this method has completely adopted the correlation of the red, green, and blue plane of a cover image and obtained high-visual-quality. Based on the literature studies, we concluded two approaches have been widely applied in steganography, one is the PVD-based approach and the other one is Least-Significant-Bit (LSB). Moreover, Farhan et al. [31] proposed a hybridization approach between steganography and cryptography for data protection, which has used particle swarm optimization algorithm (PSO) in encryption and steganography. Besides, Least Significant Bit (LSB) was applied to insert the encrypted data into LSB of the cover and the PSO was used to specify the location of concealed data.

We proposed a steganographic algorithm based on variant expansion and modulus function which illustrate stego-image of high quality in statistical as well as visual means with high embedding capacity and can be perceived in each of the three directional edges.

3. Proposed Algorithm

New information hiding techniques are always required to remove limitations or drawbacks encountered in the previous ones in order to enhance their performance. This section briefly describes the complete process of the secure stenography method for hiding the information and how the tool has been performed step by step. In this paper, our proposed approach maintains the privacy, confidentiality, and accuracy of the data by using two layers of security and presents the structure for the complete procedure of the network. The network is capable to conceal the data interior of the image as well as recovering the data from the image. For inserting the information into a picture, it requires two critical records. The first is the primary picture asserted cover-picture. The picture which is in the JPEG organization will hold the shrouded data. The second record is simply the message, which is the data to be concealed in the image.

In this way, we proposed an efficient data concealing approach that is presents data embedding and data extracting algorithms. The developed method allows confidential data to be hidden based on the variant expansion (VE) in the term of both positive and negative variance computed among pixels which is various from Mandal and Das method [29] and Shen et al. [30] that conceals secret data in smooth areas. Furthermore, we applied modulus function in order to enhance embedding capacity and increase the quality of a cover image. The high impact on embedding capacity our method has considered only positive values. Hence, the main purpose of this method is to increase the embedding capacity while maintaining a good PSNR. In this way, to improve the performance of our proposed method, we provided two scopes operations that control the embedding process. For the initial direction, we select positive values in the first scope which are among 0 and 2 ($0\leq \eta \leq 2$) while selected negative values for the second scope among -1 and -2 ($-1\geq \eta \geq -2$). Where η is applied to represent the difference value.

Furthermore, in order to make extracted algorithm straightforward, the modulus function is incorporated in the developed extraction algorithm i.e., it does recover concealed data and reduce complexity. The proposed method illustrates the functionality of the learning algorithm, which required the necessary steps to conceal and extract the secret data are shown below. In addition, the algorithms and functional capability of the proposed method are presented in Figs. 2 to 7.

3.1. Concealing the secret data

It is the first step to the information hiding technique; in this step, firstly take input the image of any dimension, and then it will be applied for embedding the secret information and secondly take a secret text that wants to securely transmission over an insecure network from one place to another. In the same way, the embedding method is one of the important parts of this proposed approach. Consequently, the whole embedding algorithm is accomplished through the subsequent strategies.

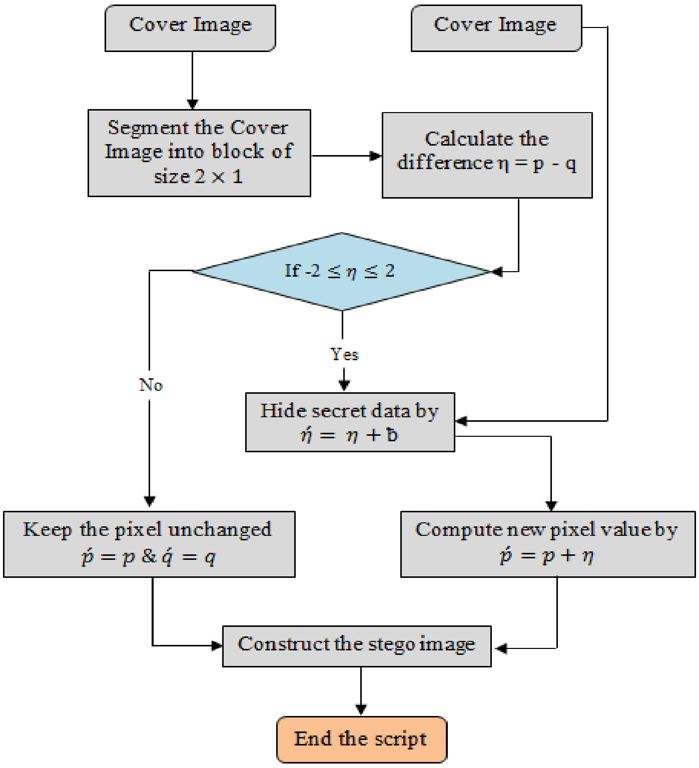

Cover Image
Cover Image
Segment the Cover Image into block of size 2 × 1
Calculate the difference η = p - q
If -2 ≤ η ≤ 2
Yes
No
Hide secret data by ή = η + ƀ
Keep the pixel unchanged ṕ = p & q́ = q
Compute new pixel value by ṕ = p + η
Construct the stego image
End the script

Fig. 2. Embedding procedure for the proposed technique.

1. Segment as a cover image into blocks of size 2 × 1.
2. After that compute the change among pixels in all values are store in each block with an array (*η_arr*) applying Eq. (1) where *p* and *q* represent the pairs of pixels in separately block however η denotes the variation having calculated.

$$\eta = p - q \tag{1}$$

3. The embedding conditions are to get entire values are satisfy throughout the array iterates, i.e., first satisfy to determine all values ($0 \leq \eta \leq 2$) and the 2nd ($-1 \geq \eta \geq -2$) situations (where these two situations modified as ($-2 \leq \eta \leq 2$).

4. Apply the tracing table (TRT), i.e., all pairs are allocated TRT variable value to distinguish. If the 1st and 2nd situations are fulfilling, the bit 0 is allocated to the value of TRT variables while the bit 1 is applied to recognize these pairs that are un-changed ("pairs having difference values which are out the range").
5. To access the confidential massage and reserve it in a text file.
6. In the third step base on the gained values, conceal the secret text by using Eq. (2) where ($\acute{\eta}$) is the modified variation, and ƀ present the secret bit to be concealed that denoted by zero or one, ƀ → $\{0,1\}$.

$$\acute{\eta} = \eta + \text{ƀ} \tag{2}$$

7. Calculate new pixel $\acute{p}$ requiring the secret bits utilizing in Eq. (3). Based on the observation this method is utilized more new pixels to build the stego image.

$$\acute{p} = \acute{\eta} + p \tag{3}$$

For embedding text, below we explain various scenarios which illustrates how the secret text is hidden inside the digital image.

1) Strategy 1: Variations η → 0 and ƀ = 1 Pixels pair p = 160, q = 160 and the secret bits ƀ → $\{0,1\}$, the variations is initially calculated utilizing Eq. (1) presented in Eq. (4).

$$\eta = 160 - 160 = 0, \quad \text{and} \quad TRT = 0 \tag{4}$$

The bit zero (0) occupied by TRT values, then the variance decreases in the dimension. Note that *TRT* values will be utilized further for capturing the difference from concealed secret bits, data applying in Eq. (2) and the new pixel is calculated to employing Eq. (3) these calculations are presented in Eqs. (5) and (6).

$$\acute{\eta} = 0 + 1 = 1 \tag{5}$$

$$\acute{p} = 160 + 1 = 161 \tag{6}$$

2) Strategy 2: Variations η → 1, *ƀ* = 1 along with *p* = 161, *q* = 160 (For the next strategies are used similar processes in Eqs. (4) to (6).

$$\eta = 161 - 160 = 1, \quad \text{and} \quad \text{TRT} = 0 \tag{7}$$

$$\acute{\eta} = 1 + 1 = 2 \tag{8}$$

$$\acute{p} = 161 + 2 = 163 \tag{9}$$

3) Strategy 3: Variations η → 2, *ƀ* = 1 along *p* = 162, *q* = 160,

$$\eta = 162 - 160 = 2, \quad \text{and} \quad \text{TRT} = 0 \tag{10}$$

$$\acute{\eta} = 2 + 1 = 3 \tag{11}$$

$$\acute{p} = 162 + 3 = 165 \tag{12}$$

4) Strategy 4: Variations η → -1, *ƀ* = 1 along *p* = 160, *q* = 161.

$$\eta = 160 - 161 = -1, \quad \text{and} \quad \text{TRT} = 0 \tag{13}$$

$$\acute{\eta} = -1 + 1 = 0 \tag{14}$$

$$\acute{p} = 160 + 0 = 160 \tag{15}$$

5) Strategy 5: Variations η → -2, *ƀ* = 0 along *p* = 160, *q* = 162

$$\eta = 160 - 162 = -2, \quad \text{and} \quad TRT = 0 \tag{16}$$

$$\acute{\eta} = -2 + 0 = -2 \tag{17}$$

$$\acute{p} = 160 - 2 = 158 \tag{18}$$

6) Strategy 6: Variations $\eta \rightarrow -2$, ƀ = 1 along $p = 106, q = 108$

$$\eta = 106 - 108 = -2, \quad \text{and} \quad TRT = 0 \tag{19}$$

$$\acute{\eta} = -2 + 1 = -1 \tag{20}$$

$$\acute{p} = 106 - 1 = 105 \tag{21}$$

For Strategies 2, 3, 4, 5 and 6, the TRT takes the value of 0 subsequently the variance value drops in the dimension. After concealing information, to become new pairs of pixel, 1st pair (p =160, q = 160) → ($\acute{p} = 161, \acute{q} = 160$), 2nd pair ($p$ = 161, q = 160) → ($\acute{p} = 163, \acute{q} = 160$), 3rd pair ($p$ = 162, q = 160) → ($\acute{p} = 165, \acute{q} = 160$), 4th pair ($p$ = 160, q = 161) → ($\acute{p} = 160, \acute{q} = 161$), 5th pair ($p$ = 160, q = 162) → ($\acute{p} = 158, \acute{q} = 162$), and 6th (p = 106, q = 108) → ($\acute{p} = 105, \acute{q} = 108$), within the secret bits ƀ → $\{111101\}$. Furthermore, to preserve new pixels value must be among the 0 and 255 in the colour level range ("new pixel → 0 ≤ new pixel ≤ 255"). The stego image and the tracing table are transferred individually to concatenates them might reduce the quality of the stego image.

3.2. Embedding data process

The proposed method is required some steps in the case of embedding algorithm, as follows:

1. In the embedding data scheme, first, separate the colour image in the form of RGB as the cover image and string the text message are presented in Fig. 3. However, the length of the text message bit should be equal to or less than the total number of pixel cover images on the RGB channel. For each partition of the colour image converts into pixel blocks contain two sequential non-overlapping pixels in the three channels (horizontal, vertical, and diagonal).

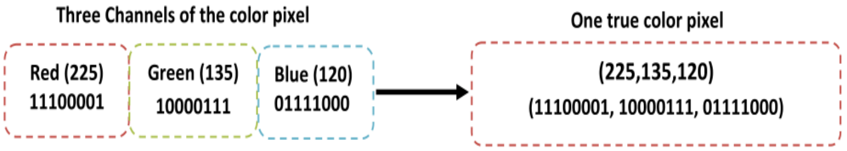
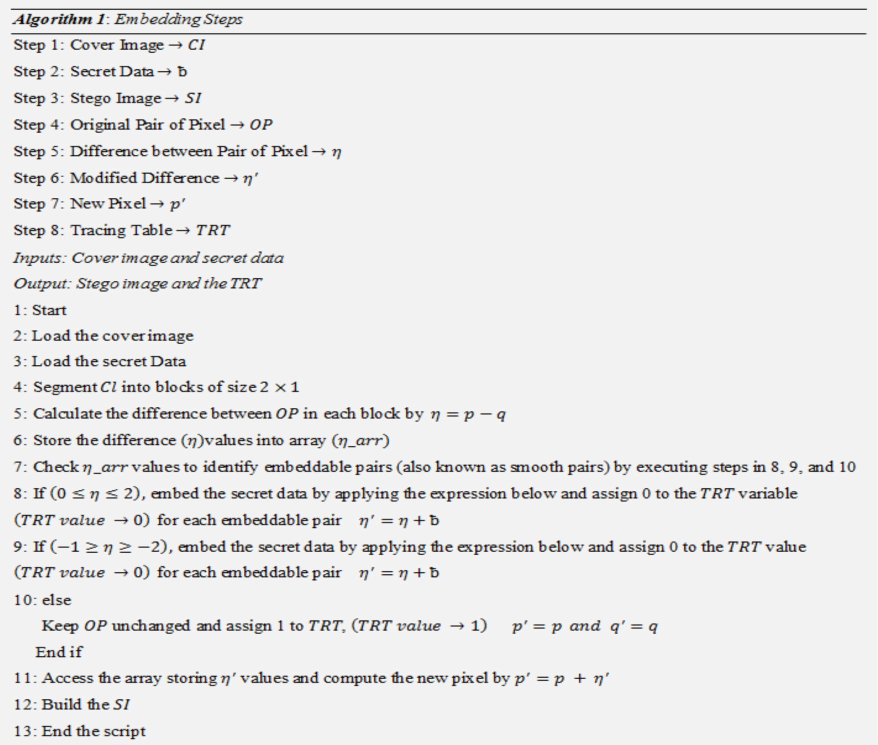


Fig. 3. Three channels strategy of a colour pixel.

2. To compute the embedding capacity (EC) of each colour channel (horizontal, vertical and diagonal) separately, and choose the embedding direction which provides the highest embedding capacity for each direction.
3. Calculate the total embedding capacity for each colour channel (Red, Green, and Blue) through Eq. (22) as follows:

$$EC = \sum_{i=1}^{3} \max\,(EC_h^i, EC_v^i, EC_d^i) \tag{22}$$

where “EC_h^i, EC_v^i and EC_d^i is the i channel embedding capacity in each direction: horizontal, vertical and diagonal respectively. Figure 4 presents the embedding algorithm for concealing the secret data.



```
Algorithm 1: Embedding Steps
Step 1: Cover Image → $CI$
Step 2: Secret Data → $\text{ƀ}$
Step 3: Stego Image → $SI$
Step 4: Original Pair of Pixel → $OP$
Step 5: Difference between Pair of Pixel → $\eta$
Step 6: Modified Difference → $\eta'$
Step 7: New Pixel → $p'$
Step 8: Tracing Table → $TRT$
Inputs: Cover image and secret data
Output: Stego image and the TRT
1: Start
2: Load the cover image
3: Load the secret Data
4: Segment $CI$ into blocks of size $2 \times 1$
5: Calculate the difference between $OP$ in each block by $\eta = p - q$
6: Store the difference $(\eta)$values into array $(\eta\_arr)$
7: Check $\eta\_arr$ values to identify embeddable pairs (also known as smooth pairs) by executing steps in 8, 9, and 10
8: If $(0 \leq \eta \leq 2)$, embed the secret data by applying the expression below and assign 0 to the $TRT$ variable
$(TRT\ value\ \rightarrow 0)$ for each embeddable pair   $\eta' = \eta + \text{ƀ}$
9: If $(-1 \geq \eta \geq -2)$, embed the secret data by applying the expression below and assign 0 to the $TRT$ value
$(TRT\ value\ \rightarrow 0)$ for each embeddable pair   $\eta' = \eta + \text{ƀ}$
10: else
    Keep $OP$ unchanged and assign 1 to $TRT$, $(TRT\ value\ \rightarrow 1)$    $p' = p\ and\ q' = q$
  End if
11: Access the array storing $\eta'$ values and compute the new pixel by $p' = p\ +\ \eta'$
12: Build the $SI$
13: End the script
```

Fig. 4. Algorithm for concealing secret data.

3.3. Recovering the concealed secret data

The extraction of the hidden data is performed using the tracing table defined during the embedding process. The stego image is initially divided by blocks of a similar range (2 by 1), subsequently, the change among pair of each pixel is calculated utilizing the Eq. (23). The concealed confidential data can be extracted by applying the modulus function and the TRT Eq. (24) when completely difference values have been achieved. Moreover, the initial portion of Eq. (25) is provided to retrieve the original pixel’s value when the TRT value is 0 otherwise it presented in the second portion of Eq. (25), the stego pixel value is equal to the original pixel’s value. Furthermore, the embedding and capturing procedures are computed to the required cover image and secret hidden data is presented by in Fig. 6 however the structure and steps for the extraction method are illustrated in Fig. 7.

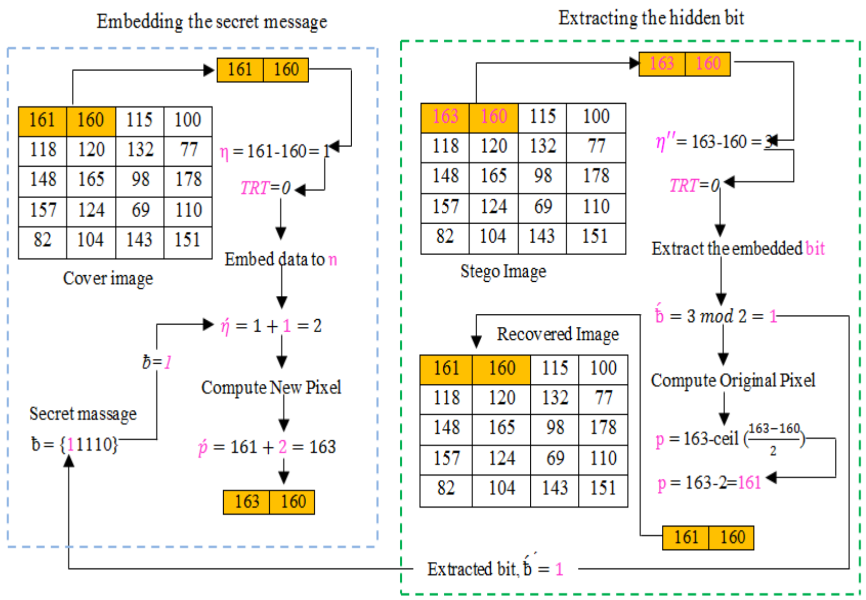
$$\eta'' = \acute{p} - \acute{q} \tag{23}$$

$$\text{ƀ} = \eta''\ mod\ 2\ if\ TRT = 0 \tag{24}$$

$$\{p = \acute{p} - \left[\frac{\acute{p}-\acute{q}}{2}\right]\ if\ TRT = 0 \qquad \text{Otherwise} \quad \{p = \acute{p}\} \tag{25}$$

where η'' is present the difference of each pixel's pair and $\acute{q}$ is refer to the hidden secret data.

In a similar process, considered the concealed text and the original pixels recovered using Eqs. (23) to (25) its implemented strategies from the first strategy to the last one (the 6th strategy) where such strategies are the opposite of the ones performed through the embedding procedure. Moreover, in below to present the similar phases in Eqs. (26) to (28) that is also used for further pairs (between strategies 2 to 6). Schematically demonstration for the embedding and extracting strategies are described in Fig. 5



161	160	115	100
118	120	132	77
148	165	98	178
157	124	69	110
82	104	143	151

163	160	115	100
118	120	132	77
148	165	98	178
157	124	69	110
82	104	143	151

161	160	115	100
118	120	132	77
148	165	98	178
157	124	69	110
82	104	143	151

Fig. 5. A block structure illustrating concealing and extraction steps applying the proposed technique.

1)Recovery strategy 1: First pair of pixels → $(\acute{p} = 161, \acute{q} = 160)$

$$\eta''= 161 - 160 = 1 \qquad (26)$$
$$TRT = 0$$

$$\acute{b} = \eta'' mod\ 2 = 1\ mod\ 2 = 1 \qquad (27)$$

$$p = 161 - \left\lceil \frac{161-160}{2} \right\rceil = 161 - \left\lceil \frac{1}{2} \right\rceil$$

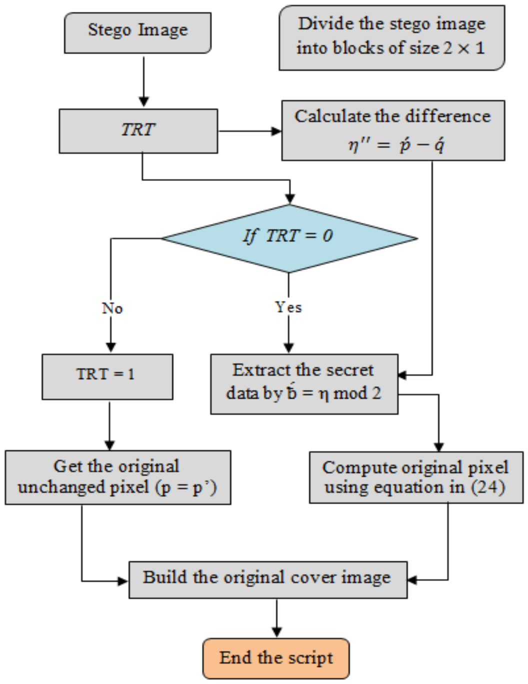
$$p = 161 - \lceil 0.5 \rceil = 160 \qquad (28)$$

2)Recovery strategy 2: Second pair of pixels → $(\acute{p} = 163,\ \acute{q} = 160)$

$$\eta'' = 163 - 160 = 3 \qquad (29)$$
$$\rightarrow TRT = 0$$

$$\acute{b} = \eta'' mod\ 2 = 3\ mod\ 2 = 1 \qquad (30)$$

$$p = 163 - \left\lceil \frac{163-160}{2} \right\rceil = 163 - \left\lceil \frac{3}{2} \right\rceil = 163 - 2 = 161 \qquad (31)$$


Stego Image
Divide the stego image into blocks of size 2 × 1
TRT
Calculate the difference $\eta'' = \acute{p} - \acute{q}$
If TRT = 0
No
Yes
TRT = 1
Extract the secret data by ƃ́ = η mod 2
Get the original unchanged pixel (p = p')
Compute original pixel using equation in (24)
Build the original cover image
End the script

3)Recovery strategy 3: Third pair of pixels → $(\acute{p} = 165,\ \acute{q} = 160)$

$$\eta'' = 165 - 160 = 5 \tag{32}$$

→ $TRT = 0$

$$ƃ́ = \eta'' mod\ 2 = 5\ mod\ 2 = 1 \tag{33}$$

$$p = 165 - \frac{165-160}{2} = 163 - \frac{5}{2} = 165 - 3 = 162 \tag{34}$$

4)Recovery strategy 4: Fourth pair of pixels → $(\acute{p} = 160,\ \acute{q} = 161)$

$$\eta'' = 160 - 161 = -1 \tag{35}$$

→ $TRT = 0$

$$ƃ́ = \eta'' mod\ 2 = abs(-1)\ mod\ 2 = 1 \tag{36}$$

$$p = 160 - \frac{160-161}{2} = 160 - \frac{-1}{2} = 160 - [-0.5] = 160 - 0 = 160 \tag{37}$$

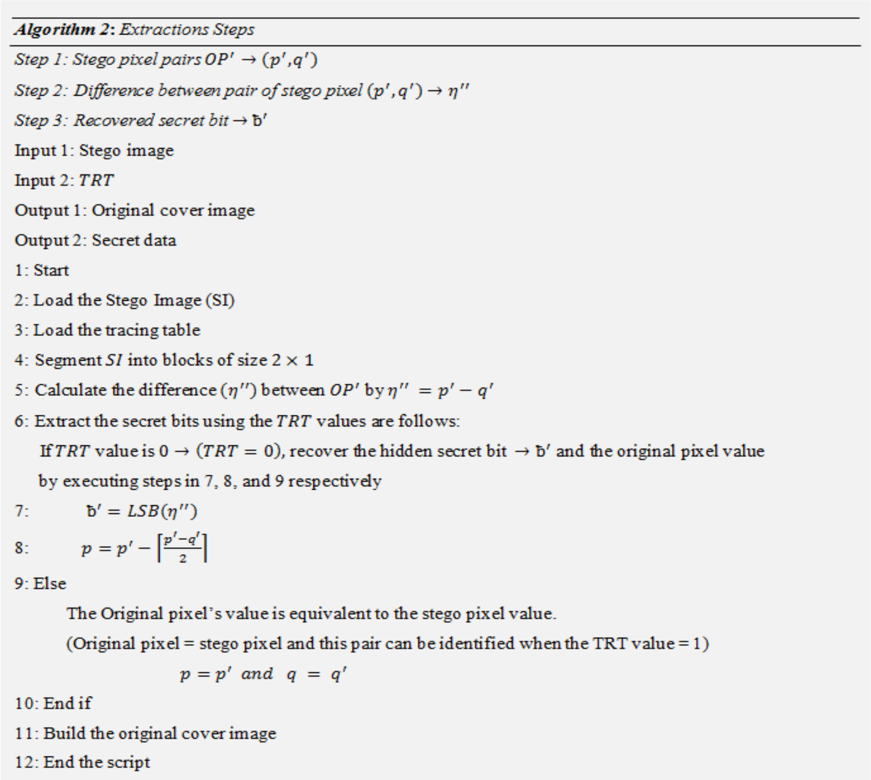
5)Recovery strategy 5: Fifth pair of pixels → $(\acute{p} = 158,\ \acute{q} = 162)$

$$\eta'' = 158 - 162 = -4 \tag{38}$$

→ $TRT = 0$

$$ƃ́ = \eta'' mod\ 2 = abs(-4)\ mod\ 2 = 0 \tag{39}$$

$$p = 158 - \frac{158-162}{2} = 158 - [\frac{-4}{2}] = 158 - -[2] = 160 = 158 + 2 = 160 \tag{40}$$



```
Algorithm 2: Extractions Steps
Step 1: Stego pixel pairs $OP' \rightarrow (p',q')$
Step 2: Difference between pair of stego pixel $(p',q') \rightarrow \eta''$
Step 3: Recovered secret bit → ƀ'
Input 1: Stego image
Input 2: $TRT$
Output 1: Original cover image
Output 2: Secret data
1: Start
2: Load the Stego Image (SI)
3: Load the tracing table
4: Segment $SI$ into blocks of size $2 \times 1$
5: Calculate the difference $(\eta'')$ between $OP'$ by $\eta'' = p' - q'$
6: Extract the secret bits using the $TRT$ values are follows:
   If $TRT$ value is 0 → $(TRT = 0)$, recover the hidden secret bit → ƀ' and the original pixel value
   by executing steps in 7, 8, and 9 respectively
7:         ƀ' $= LSB(\eta'')$
8:         $p = p' - \left\lceil \frac{p'-q'}{2} \right\rceil$
9: Else
       The Original pixel's value is equivalent to the stego pixel value.
       (Original pixel = stego pixel and this pair can be identified when the TRT value = 1)
                   $p = p'\ and\ \ q = q'$
10: End if
11: Build the original cover image
12: End the script
```

6)Recovery strategy 6: Sixth pair of pixels → $(\acute{p} = 105,\ \acute{q} = 108)$

$$\eta'' = 105 - 108 = -3 \qquad (41)$$

→ $TRT = 0$

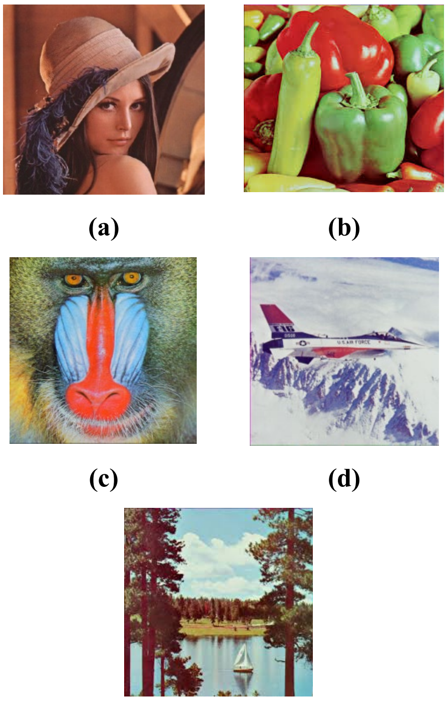
$$ƀ́ = \eta'' mod\ 2 = abs(-3)\ mod\ 2 = 1 \qquad (42)$$

$$p = 101 - \frac{105-108}{2} = 101 - [\frac{-3}{2}] = 101 - (-[1.5]) = 101 + 1 = 102 \qquad (43)$$

The ceiling brackets “[*p*] permit to the round integer value of *p* is greater than or equivalent to *p* although the floor brackets [*p*] round the value of *p* to the closest integer less than or equivalent to *p*. For the extraction of hidden confidential data from the stego-image by implementing the following steps are described in Fig. 7. The extracted secret bits in (27), (30), (33), (36), (39) and (42), ƀ →{111101} and the values of the recovered pixels in (28), (31), (34), (37), (40) and (43) are accurately similar as the original ones. That is, the concealed confidential data and the original cover image can be regained without any differences or distortion.

4. Experimental Results and Discussion

In this experimental section, we conducted experiment on colour images by using variant expansion and modulus function and the different simulations were performed to evaluate the performance of the proposed method. A set of RGB images has been applied for this objective. All the experiments of the proposed method were implemented on a personal computer with specifications (Intel Core i7-3770XPU on a Windows PC with @3.40 GHz, and 4GB RAM machine with window 7 operating system) and using MATLAB version 2012(a). To illustrate the performance of the proposed method for hiding secret data in RGB channels of the stego-image. For research and experimental purposes, we used five colour images of different categories as cover images size 512×512 were selected from the SIPI image database are included Lena, Peppers, Baboon, Airplane, Sailboat" are presented in Fig. 8. The performance comparison is evaluated based on determining the PSNR values, embedding capacity, NPCR, UACI, and pixel difference histogram analysis.



(a) (b)

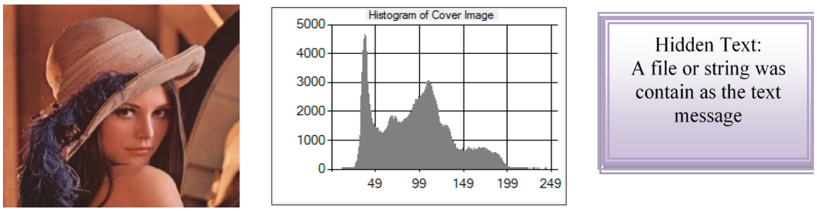
(c) (d)

(e)

Fig. 8. Standard 512 x 512 cover images used in experiments (a) Lena (b) Peppers (c) Baboon (d) Airplane (e) Sailboat.

4.1. Pixel difference histogram analysis

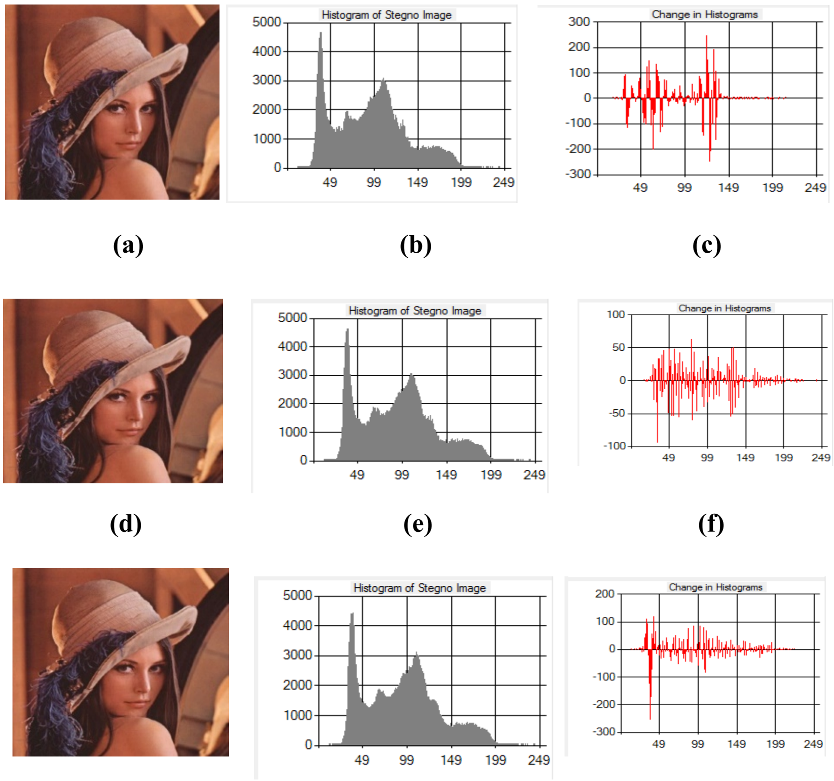
A pixel difference histogram is one of the most effective stego-analysis methods to reveal the confidential data of stego-images. The pixel difference histogram is calculated by adopting the differences of neighbouring pixels with fall-off series among cover and stego-image. Figs. 9(a) - (i) are illustrated to provide the example of the cover image histogram before and after hiding data. Fig. 9(a) presents the pixel difference histogram of the cover bitmap Lena image by using the proposed method, and Fig. 9(b) presents its histogram of the cover image while a "TEXT" file is presented in Fig. 9(c), which was applied to embed into the cover image. Similarly, Fig. 10(a) shows the image after embedding the data into it by the sequential pixel selection with modulus function and variant expansion method. Fig. 10(b) shows the histogram of Fig. 10(a). It is visually perceivable from the Fig. 9(a) and Fig. 10(a) and their respective histograms shown in Fig. 9(b), and Fig. 10(b) that there is a minor difference in an image that is not easily interpretable by the human eye. However, there is some change in image quality after embedding of text into it. To verify the extent of change in the image after steganography, we calculated the difference between them and visualized the difference in Fig. 10(c) represented by red lines.



Hidden Text:
A file or string was contain as the text message

(a) **(b)** **(c)**

Fig. 9. (a) Original BMP Portrait Image (Lena)
(b) Histogram of the image and (c) The text file to hidden in the image.



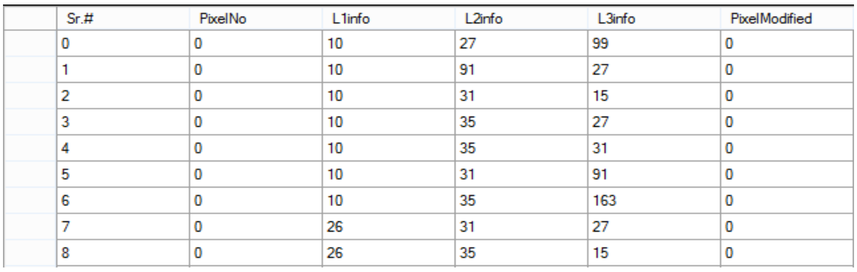
(a) **(b)** **(c)**

(d) **(e)** **(f)**

(g) **(h)** **(i)**

Fig. 10. (a), (d) and (g) illustrated the Stego CG Image,
while Fig. 10 (b), (e) and (h) present the histogram of the image,
and Fig. 10 (c), (f) and (i) change in stego image represented by red lines.

This is the actual change that occurred in cover image after steganography using the sequential ordering of storing data into pixels on LSB one character per pixel. Data was embedded into an image with the format as 3 bits at RED component, 3 bits at GREEN component and 2 bits of BLUE component of each sequentially selected pixel. Resultantly, no change occurred even in a single pixel of the cover image. Rather, a pattern selection technique is applied for extracting the bit pattern of characters from the byte values of different colour components of the pixel. The extracted information is saved into a LOG table as shown in Fig. 10(p). Therefore, our proposed method gives more security over maintaining the pixel difference histogram close to the cover-image; it did not produce any perceivable artifacts under pixel difference histogram stego-analysis detection attacks.



Sr.#	PixelNo	L1info	L2info	L3info	PixelModified
0	0	10	27	99	0
1	0	10	91	27	0
2	0	10	31	15	0
3	0	10	35	27	0
4	0	10	35	31	0
5	0	10	31	91	0
6	0	10	35	163	0
7	0	26	31	27	0
8	0	26	35	15	0

Fig. 11.Extracted information from the byte values of different colour components of the pixel.

4.2. MSE and PSNR based analysis

To evaluate the performance of the proposed method with state-of-the-art existing approaches by using different parameters. Four images with (512x512) size are applied as cover images (Lena, Peppers, Baboon, Airplane, Sailboat) have presented in Fig. 8 for illustration purposes. The Peak Signal to noise ratio (PSNR) and MSE is the standard measurement in order to assess the difference between the original cover image and the stego-image.

We investigated the embedding capacity and PSNR performance of the proposed method by using three embedding directions of the stego-image for each colour channel (“R, G, and B). In this research, we have overcome the major drawback that was addressed in the previous PVD-based steganography method is low embedding capacity by using various embedding directions. The experimental results of the proposed method in the term of embedding direction capacity along with each colour channel R, G and B are shown in Table 1. Based on the achieved results, we can notice that the highest embedding capacity has been obtained by diagonal direction as compared to two other directions. This is happening due to low correlation between diagonal pixels compared with the high correlation pixels lie in the vertical and horizontal directions. The performance of the proposed method on the colour image is evaluated in various aspects. First, we noticed that our proposed method obtained the highest embedding capacity of the diagonal direction as compared with the other two directions. Second, in the case of the vertical direction, the proposed method gives better PSNR value as compared to the other two directions which provide more security for the stego-images and lead to better visual quality.

Table 1. The results of the proposed method in terms of hiding capacity for colour images.

Cover image	Red capacity			Green capacity			Blue capacity		
512 x 512 (colour)	**H**	**V**	**D**	**H**	**V**	**D**	**H**	**V**	**D**
Lena	421158	415786	**427862**	421768	413587	**425911**	423158	420158	**428835**
Pepper	405268	416954	**419835**	382147	379960	**385469**	375486	386574	**390247**
Baboon	441268	436785	**452368**	475724	468435	**476725**	464867	471287	**481349**
Airplane	406825	406214	**411965**	419654	425139	**428620**	412954	412568	**414837**
Sailboat	422598	426567	**429512**	404761	399750	**408647**	425236	421289	**429553**

High PSNR value shows that the cover image has a small distortion after embedding. Low PSNR value presents a poor visual quality of the cover image. The calculation formulas of *PSNR* and *MSE* are defined in Eqs. (44) and (45).

$$PSNR = 10log_{10}(\frac{255^2}{MSE}) \tag{44}$$

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[I(x,y)-I^{*}(x,y)]^2}{M \times N} \tag{45}$$

where *M* and *N* represent the length and width of the image, and I(x, y), I*(x, y) respectfully stand for the original pixel value and the stego-pixel value at position (x, y).

Similarly, the experimental results of the proposed method in the terms of PSNR value for embedding direction are shown in Table 2. According to the value of Table 2, we observed that the overall PSNR value greater than 45 dB, while presents the superior imperceptibility of original images after the secret data is embedded in them. At this level, the visual appearance of the stego-images seems to be better while the changes in the cover image according to embedding secret data are hard to be recognized or detected by the human vision. In general, the developed method can be extremely useful in a situation where small or medium embedding capacity is needed.

Table 2. Performance of the proposed method in terms of PSNR for embedding direction.

Cover image 512 × 512 (Colour)	Horizontal PSNR (dB)	Vertical PSNR (dB)	Diagonal PSNR (dB)
Lena	53.96	**54.74**	52.34
Pepper	52.47	**52.68**	51.81
Baboon	49.57	**46.37**	46.13
Airplane	54.75	**54.08**	53.17
Sailboat	53.14	**53.21**	52.95

4.3. Comparison of proposed method with existing approaches

In this research, we conducted evaluation comparison performance of the proposed method with well-known approaches included, Mandal and Das [29], Shen et al. [30], Hussain et al. [31] and Rajendran and Doraipandian [32] methods. For comparison purposes, in this experiment, we used five colour images (Lena, Pepper, Baboon, Airplane, Sailboat) are presented in Fig. 10. The performance of proposed method in the term of PSNR and compared with existing methods are presented in Table 3, while MSE performance of the proposed method with existing

Hussain et al. [31] and Rajendran and Doraipandian [32] methods have implemented to achieved for comparison are given in Table 4.

The proposed method has achieved much better results in the term of PSNR and MSE as compared to existing state-of-the-art methods. The experimental results using colour images illustrate that the proposed method gives better visual quality and embedding capacity than other existing approaches such as Mandal and Das [29] and Shen et al. [30] in together diagonal and vertical directions are summarized in Table 3.

Table 3. Performance comparison of our proposed method with the existing methods using colour images.

Cover Images	Mandal and Das Method		Shen et al. Method		Proposed Method			
					Vertical		Diagonal	
512 x 512 (Colour)	Capacity bits	PSNR dB	Capacity bits	PSNR dB	Capacity bits	PSNR dB	Capacity bits	PSNR dB
Lena	1,166,296	42.26	810757	37.13	1,226,351	**54.74**	**1,263,354**	52.34
Pepper	1,167,960	42.28	812986	36.74	1,171,584	**52.68**	**1,185,126**	51.81
Baboon	1,159,328	38.44	918877	34.94	1,382,657	**46.37**	**1,420,631**	46.13
Airplane	1,165,184	42.6	818887	36.35	1,219,880	**54.08**	**1,253,349**	53.17
Sailboat	1,163,273	40.66	851837	36.03	1,186,542	**53.21**	**1,203,410**	52.08

According to the obtained results, it can be notable that the stego-image is visually undetectable from their original ones through human eyes. On the other hand, for the evaluation of mean square error we compared our proposed method with state-of-the-are existing methods (i.e., Hussain et al. [31] and Rajendran and Doraipandian [32]) are shown in Table 4. The proposed method shows superior performance in the terms of PSNR values, MSE, and hiding capacity as compared to existing methods.

Table 4. Performance comparison in the term of (MSE) with existing methods

Parameter	**Methods**	**Images**			
		Lena	**Peppers**	**Baboon**	**Airplane**
MSE	Hussain et al., [30]	2.61	2.98	2.91	2.79
	Rajendran et al., [31]	2.28	2.58	2.28	2.34
	Proposed	1.89	2.19	2.06	1.74

4.4. NPCR and UACI

A good image encryption method must be resistant to the differential attack, which needs that a slight alteration in the colour image. The NPCR (Number of pixels Change Rate) and UACI (Unified Average Changing Intensity) can be used to measure the sensitivity of the encryption method to plaintext, which is an important indicator to test the number of changing pixels and the number of averaged changed intensity between the ciphertext images respectively. Here, Eq. (46) and Eq. (47) are calculating NPCR and UACI of three components [34] (R, G and B components):

$$NPCR_{R,G,B} = \frac{1}{W\times H}\sum_{i,j} D_{R,G,B}(i,j) \times 100\% \tag{46}$$

$$UACI_{R,G,B} = \frac{1}{W\times H}\left\{\sum_{i,j}\frac{C_{R,G,B}(i,j) - \bar{C}_{R,G,B}(i,j)}{255}\right\} \times 100\% \tag{47}$$

where W and H refer to the width and height of the image respectively, $C_{R,G,B}$ and $\bar{C}_{R,G,B}$ illustrate the corresponding cipher image pixel values before and after one pixel is variation respectively. For the pixel at positioni, j, if $C_{R,G,B}(i,j) \neq \bar{C}_{R,G,B}(i,j)$,let $D(i,j) = 1$; else let $D(i,j) = 0$. (The comparison between some tested original images and ciphered images are illustrated in Table 5. It is observed that the proposed method obtained better results as compared to existing methods. The UACI measures the average intensity of differences between the original image and ciphered images or stego-image, the result of UACI for stego-image should be near to zeroes while for the ciphered image should be between 32 and 33. Table 5 presented the values of UACI and NPCR for a ciphered image, it can be demonstrated that the NPCR results of the proposed method are near to 100% and the UACI results are near to 33-34 [35], which displays that the proposed technique is highly sensitive to the little variation of the colour image and then can resist differential attack. Change randomly the pixel values of each component, the test is performed 20 times, and the achieved average NPCR and UACI of R, G, B components for various plain images for our proposed method and the method [36] and the method [37] are presented in Table 5.

Table 5. Comparison of NPCR and UACI for colour images.

Methods	Cover image	*NPCR* (%)			*UACI* (%)		
	512×512 (colour)	R	G	B	R	G	B
Proposed Method	Lena	99.8117	99.8134	99.8104	33.4155	33.3961	33.4067
	Pepper	99.8199	99.8129	99.8095	33.3835	33.3659	33.4269
	Baboon	99.8208	99.8177	99.8024	33.4295	33.3198	33.3149
	Airplane	99.8178	99.8195	99.8051	33.4018	33.3825	33.4058
Wang and Zhang Method [35]	Lena	99.6124	99.6134	99.6192	33.4438	33.5232	33.5010
	Pepper	99.6200	99.6105	99.6164	33.4451	33.3776	33.4782
	Baboon	99.6024	99.6017	99.6052	33.4273	33.4432	33.4471
Boopathy and Sundaresan Method [36]	Lena	99.8039	99.8017	99.8097	33.3796	33.3886	33.3988
	Pepper	99.8166	99.8073	99.8199	33.3013	33.2930	33.4362
	Baboon	99.8146	99.8164	99.8012	33.3569	33.2790	33.2897

5. Conclusions

In this research work, we proposed a secure steganographic method for the secure transmission of data hiding by using variant expansion and modulus function. Moreover, variant expansion (VE) is one of the common reversible schemes of data hiding because of its capability of reversibly recovering the secret data and the original cover image without degradation. Based on the VE-based scheme, the modulus function permits the secret data to be hidden into a digital image and calculates the difference of confidential data among pixel pairs in each block. Five different colour images were tested to demonstrate the proposed method using PSNR values, embedding capacity, "NPCR, UACI, and pixel difference histogram analysis. In addition, the proposed method partitioned the literal of text into three literals and searched for their patterns in pixel components based on difference modulus function. After successful matching of text message character bits, the findings are packed into bytes and are stored in a LOG table. The LOG table is then encrypted using Rijndael Managed encryption algorithm for added security when sent on the communication channel. LOG table works as a secret key. The experimental results illustrated that our method not only has certain flexibility in adjusting the trade-off between hiding capacity and stego-image quality," but also gives higher hiding capacity and more satisfied visual quality of the stego-images compared with state-of-the-art methods.

Nomenclatures

ƀ	Secret bit
$\acute{p}$	New pixel
$p - q$	Pairs of pixels
$\acute{q}$	Hidden secret data

Greek Symbols

η	Variance of calculated
$\acute{\eta}$	Modified difference
η''	Present the difference of each pixel's

Abbreviations

EA	Embedding Algorithm
EC	Embedding Capacity
EXA	Extraction Algorithm
LSB	Least Significant Bit
NPCR	Number of pixels Change Rate
RGB	Red, Green, Blue
SI	Stego Image
TRT	Tracing Table
TPVD	Tri-way Pixel Value Differencing
UACI	Unified Average Changing Intensity
VE	Variant Expansion

References

1. Ibrahim, R.; and Kuan, T.S. (2011). Steganography algorithm to hide secret message inside an image. *Computer Technology and Application,* 8(2),102-108.
2. Bandyopadhyay, S.K.; Bhattacharyya, D.; Ganguly, D.; Mukherjee, S.; and Das, P. (2008). A tutorial review on steganography. *Proceedings of the International Conference on Contemporary Computing*. Noida, India, 105-114
3. Uddin, M.P.; Saha, M.; Ferdousi, S.J.; Afjal, M.I.; and Marjan, M.A. (2014). Developing an efficient solution to information hiding through h text steganography along a with cryptography. *Proceedings of the 9th International Forum on Strategic Technology.* Cox's Bazar, Bangladesh, 14-17.
4. Hameed, M.A.; Aly, S.; and Hassaballah, M. (2018). An efficient data hiding

method based on adaptive directional pixel value differencing (ADPVD). *Multimedia Tools and Applications*, 77(12), 14705-14723.

5. Takano, S.; Tanaka, K.; and Sugimura, T. (2000). Data hiding via steganographic image transformation. *IEICE Transactions on Fundamental*, E83-A(2), 311-329.
6. Ansari, A.S.; Mohammadi, M.S.; and Parvez, M.T. (2019). A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security,* 1, 11-25.
7. Sahu, A.K.; and Swain, G. (2019). Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis. *International Journal of Electronic Security and Digital Forensics,* 11(4), 458-476.
8. Kumari, P.; Kumar, C.; and Bhushan, J. (2013). Data security using image steganography and weighing its techniques*. International Journal of Scientific and Technology Research,* 2(11), 238-241.
9. Cao, F.; An, B.; Yao, H.; and Tang, Z. (2019). Local complexity based adaptive embedding mechanism for reversible data hiding in digital images. *Multimedia Tools and Applications*, 78(7), 7911-7926.
10. Subhedar, M.S.; and Mankar, V.H. (2014). Current status and key issues in image steganography: A survey. *Computer Science Review*, 13-14, 95-113.
11. Saleema, A.; and Amarunnishad, T. (2016). A new steganography algorithm using hybrid fuzzy neural networks. *Procedia Technology,* 24, 1566-1574.
12. Cheddad, A.; Condell, J.; Curran, K.; and Kevitt, P.M. (2008). Enhancing steganography in digital images. *Proceedings of the Canadian Conference on Computer and Robot Vision.* Windsor, Canada, 326-332.
13. Sahu, A.K.; and Swain, G. (2018). Digital image steganography using PVD and modulo operation. *Internetworking Indonesia Journal*, 10(2), 3-11.
14. Cheddad, A.; Condell, J.; Curran, K.; and Kevitt, P.M. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3), 727-752.
15. Chen, J. (2014). A PVD-based data hiding method with histogram preserving using pixel pair matching. *Signal Processing: Image Communication*, 29(3), 375-384.
16. Li, X.; Li, B.; Luo, X.; Yang, B.; and Zhu, R. (2013). Steganalysis of a PVD-based content adaptive image steganography. *Signal Processing*, 93(9), 2529-2538.
17. Zielińska, E.; Mazurczyk, W.; and Szczypiorski, K. (2014). Trends in steganography. *Communications of the ACM*, 57(3), 86-95.
18. Wu, D.-C.; and Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9-10), 1613-1626.
19. Wang, C.-M.; Wu, N.-I.; Tsai, C.-S.; and Hwang, M.-S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, 81(1), 150-158.
20. Chang, K.-C.; Chang, C.-P.; Huang, P.-S.; and Tu, T.-M. (2018). A novel image steganographic method using tri-way pixel-value differencing. *Journal of Multimedia*, 3(2), 37-44.
21. El-sayed, H.S.; El-Zoghdy, S.F.; and Faragallah, O.S. (2016). Adaptive difference expansion-based reversible data hiding scheme for digital images.

Arabian Journal for Science and Engineering, 41, 1091-1107.

22. Chen, H.; Ni, J.; Hong, W.; and Chen, T.-S. (2016). Reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering. *Signal Processing: Image Communication*, 46, 1-16.
23. Arham, A.; Nugroho, H.A.; and Adji, T.B. (2017). Multiple layer data hiding scheme based on difference expansion of quad. *Signal Processing*, 137, 52-62.
24. Peng, F.; Li, X.; and Yang, B. (2012). Adaptive reversible data hiding scheme based on integer transform. *Signal Processing*, 92(1), 54-62.
25. Sahu, A.K.; and Swain, G. (2020). Reversible image steganography using dual-layer LSB matching. *Sensing and Imaging*, 21(1), 1-21.
26. Arham, A.; Nugroho, H.A.; and Adji, T.B. (2016). Combination schemes reversible data hiding for medical images. *Proceedings of the 2nd International Conference on Science and Technology-Computer*. Yogyakarta, Indonesia, 44-49.
27. Sahu, A.K.; and Swain, G. (2018). Pixel overlapping image steganography using PVD and modulus function. *3D Research*, 9(3).
28. El-Emam, N.N.; and Al-Zubidy, R.A.S. (2013). New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm. *Journal of Systems and Software*, 86(6), 1465-1481.
29. Mandal, J.K.; and Das, D. (2012). Colour image steganography based on pixel value differencing in spatial domain. *International Journal of Information Sciences and Techniques*, 2(4), 83-93.
30. Shen, S.; Huang, L.; and Tian, Q. (2015). A novel data hiding for colour images based on pixel value difference and modulus function. *Multimedia Tools and Applications,* 74(3), 707-728.
31. Hussain, M.; Wahab, A.W.A.; Javed, N.; and Jung, K.-H. (2016). Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. *Symmetry*, 8(6), 1-21.
32. Rajendran, S.; and Doraipandian, M. (2017). Chaotic map based random image steganography using LSB technique. *International Journal of Network Security,* 19(4), 593-598.
33. Farhan, A.K.; Ali, R.S.; and Ali, S.M. (2019). Secure location MAP and encryption key based on intelligence search algorithm in encryption and steganography to data protection. *International Journal of Mechanical Engineering and Technology,*10(1), 8-24.
34. Ahmad, J.; Hwang, S.O.; and Ali, A. (2015). An experimental comparison of chaotic and non-chaotic image encryption schemes. *Wireless Personal Communications*, 84(2), 901-918.
35. Wang, X.; and Zhang, H.-L. (2015). A colour image encryption with heterogeneous bit-permutation and correlated chaos. *Optics Communications*, 342, 51-60.
36. Boopathy, D.; and Sundaresan, M. (2019). A novel multi-dimensional encryption technique to secure the grayscale images and colour images in public cloud storage. *Innovations in Systems and Software Engineering,* 15(1), 43-64.
37. Seyedzadeh, S.M.; and Mirzakuchaki, S. (2012). A fast colour image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Processing*, 92(5), 1202-1215.