Journal of King Saud University – Computer and Information Sciences 31 (2019) 335–347

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Information hiding scheme for digital images using difference expansion and modulus function

Pascal Maniriho, Tohari Ahmad *

Department of Informatics, Institut Teknologi Sepuluh Nopember (ITS), Kampus ITS Keputih Sukolilo, Surabaya 60111, Indonesia

ARTICLE INFO

Article history:
Received 20 November 2017
Revised 30 January 2018
Accepted 31 January 2018
Available online 2 February 2018

Keywords:
Confidential data
Data hiding
Data protection
Difference expansion
Information security

ABSTRACT

Disguising the presence of communication has become a severe concern in this highly digitalized world due to the unauthorized data access and network policy violations that are emerging rapidly. These issues have led to the application of cryptography technique as a mean for securing data by encrypting them. However, since the encrypted data can be seen by sophisticated intruders during the transmission, this may lead to its suspicion which can results in unauthorized access. Thereby, steganography is another technique for securing communication. Steganography is the practice of concealing confidential information in the codes that make up digital files. Different from encryption, however, steganography provides security by disguising the presence of communication. In this context, this paper presents an improved information hiding implemented based on difference expansion and modulus function. The previous method has only considered the image smooth areas where the difference value is 0 or 1 while ignoring other values for hiding data. These limitations may result in decreasing the embedding capacity for all images having few smooth areas. Hence, a new scheme that considers both positive and negative difference values to conceal secret data is developed. The experimental results prove that the proposed scheme achieves better results than the existing methods.

1. Introduction

In security systems, information hiding is a broad discipline that encompasses a comprehensive range of several research areas. The word "hiding" refers to safeguarding confidential information through unknown communication (Khandelwal et al., 2015). Cryptography and steganography are one of the research fields in information security that had been around for several years. However, even though both technologies aim at protecting confidential data, they do possess different concepts. Cryptography involves protecting communication by encrypting data before being sent or shared without hiding the communication existence, i.e., the third party (intruders or unauthorized party) can see the encrypted data while being transmitted to the destination which may lead to its suspicion and interception. In contrast to the cryptography, steganography is the practice of hiding information in the codes that make up digital files such as audio, text, image or video while preventing unwanted sources from discovering the communication presence. That is, data transmission is kept confidential between the intended communicating parties. This ensures that the data protection is well maintained which is a necessity in any types of communication.

A well designed steganographic system is made up of three principal parts namely, transmitter, communication channel and the recipient. The transmitter is the party that conveys confidential data and the recipient is the party that the data are intended to while the channel assists in conveying data. In digital image steganography, confidential data can be concealed in the appropriate cover image. The output is the stego image which can be directly transferred across an unsecured public network (Fig. 1 is provided to illustrate this concept).

Besides, due to the high degree of redundancy encountered in digital image, several steganographic methods that hides data in digital images have been already presented in the literature (Subhedar and Mankar, 2014). A method where pixels for hiding secret data are selected randomly was suggested by Saleema and Amarunnishad (2016) and the hybrid fuzzy neural networks was

* Corresponding author.
E-mail addresses: pascal15@mhs.if.its.ac.id (P. Maniriho), tohari@if.its.ac.id (T. Ahmad).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2018.01.011
1319-1578/© 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

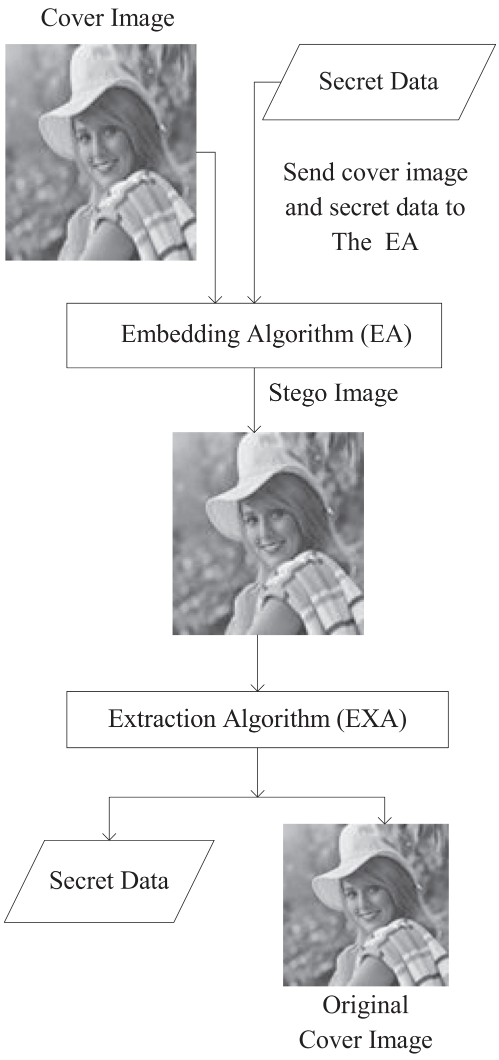


Fig. 1. Reversible digital image steganography.

used to perform the post processing of the stego media. Cheddad et al. (2008) implemented an adaptive method that embeds data in regions of interests of the cover image. In 2017, Han et al. introduced a new model aiming to incorporate steganography into cybersecurity (Han et al., 2017). The visual quality of the stego image was enhanced in the scheme that uses 2-bit identical technique and optimal pixel adjustment procedure presented by Kaur and Goel (2015). Before concealing the secret data, the cover image was split up into blocks and the data to be concealed were segmented into segments. Their technique has greatly improved the perceptibility since data were hidden into blocks with less effect on the visual quality of the stego image.

In further research, the embedding positions have to be selected based on smooth and edge areas before concealing data (Li et al., 2017). To maintain the security of data, secret sharing and steganography were applied to implement the approach that embeds data into images (Rajput et al., 2016). Discrete wavelet transform (DCT) was employed to build a blind steganographic method suggested by Bugár et al. (2014). Being blind means that the original cover image is not required to extract the hidden data which makes the data transmission undetectable by any unauthorized parties. Furthermore, to enhance the visual quality the Huffman code was used to encode the message. By employing integer transform, an adaptive reversible information hiding was provided by Peng et al. (2012). The median was utilized as the base point by Yaqub and Al-jaber to enhance the DE-based vector (Yaqub and Al-jaber, 2006). In the reversible data hiding method (RDH) model presented by Zhang et al. (2014), the histogram shifting technique was applied to shift the predicted error encrypted histogram. In the RDH models based on digital image the same original cover image and the embedded data can be thoroughly retrieved after the extraction phase. Additionally, the RDH methods are recognized among the best methods applied in the situation like satellite and medical images to provide authentication, user privacy, content and copyright protection (El-sayed et al., 2016). The large smooth areas are one of the well-known characteristics of medical images. This property permits secret data to be concealed with less distortion of the stego image (Arham et al., 2016). That is, the stego media cannot be easily suspected by malicious users. This paper intends to suggest a new difference expansion (DE) and modulus function-based data hiding scheme that improves the embedding capacity. In addition, the modulus function is employed during the extraction phase to recover the hidden confidential data. The main goal is to increase the embedding capacity while still maintaining a reasonable quality of the stego image. Furthermore, it is worth noting that the proposed scheme is implemented in the spatial domain.

The following sections will be presented in the next parts of this paper. First of all, the literature study is provided in Section 2 thereafter the proposed method is elucidated in Section 3 while Section 4 gives the results and discussion. To wrap up the paper, the conclusion is given in Section 5.

2. Current trends in digital image-based data hiding methods

Due to various technologies incorporated in digital image steganography in the recent years, there is a great achievement in terms of performance, i.e., intelligent algorithms allowing to secure secret information have emerged. Based on the application domain, these algorithms can be broadly categorized into spatial domain and transform (frequency) domain techniques. Concealing confidential data in the spatial domain is carried out by directly manipulating the pixel values of the cover image in order to achieve the desired improvement (El-sayed et al., 2016). More importantly, techniques such as least significant bit (LSB) (Verma et al., 2014; Malik et al., 2015; Yang, 2008), difference expansion (Arham et al., 2017; Al-qershi and Khoo, 2011), histogram shifting (Yin et al., 2016; Chen et al., 2016), pixel value modification (PVD) (Nagaraj et al., 2013) and integer transform (Peng et al., 2012; Alattar, 2004) are used in the spatial domain. These approaches are mostly employed when a direct alteration of specific or all image pixel values is required. Moreover, they achieve a high embedding capacity but they are sometimes prone to low quality of the stego image. Difference expansion has become among the most famous spatial domain algorithms. It enables secret data to be concealed by extending the difference values calculated between pixels.

Arham et al. (2016) presented a reversible data hiding method that hides data in medical images while maintaining both quality of the stego image and the payload capacity. To conceal data in binary encrypted images, the binary block embedding (BBE) was employed. Moreover, a new security key design approach was introduced to make the proposed algorithm to be able to resist to the data loss, brute-force, noise, differential and attacks. This scheme is completely reversible and it allows the embedded secret data to be restored independently without any loss (Yi and Zhou, 2016). A new secret-key sharing approach aiming to secure confidential data was proposed in Gutub (2017). Secret message was hidden in the low-bits of RGB image (Rahmani and Mohammad, 2017). An adaptive algorithm that utilizes the partition scheme to determine the secret data bits that can be disguised in each pixel of the carrier image without causing substantial degradation was presented in Parvez and Gutub (2014). Nouf and Gutub 's data hiding scheme allows the user to easily choose the best suitable cover image for embedding data based on the desired security priorities (Al-otaibi and Gutub, 2014a). To improve the performance of DE-based method, Al-qershi and Khoo (2011) had implemented two schemes by combining the existing ones. The first approach was developed by combining Tian's approach (Tian, 2003) with the one in (Chiang et al., 2008), while for the second approach, Alattar's and Chiang's et al. approaches (Alattar, 2004; Chiang et al., 2008) were combined together. The experimental results demonstrate that both schemes achieve high embedding capacity and good visual quality especially for medical images. By applying histogram modification, a reversible information hiding approach was developed by Tsai et al. (2013). The histogram was constructed using values generated by calculating the difference between neighboring pixels, thereafter it was used to locate all pixels that are at the peak in order to be used for hiding secret data. Besides, this approach is highly applicable for grayscale images. Confidential data were embedded in audio and video files (Andra et al., 2017; Firmansyah and Ahmad, 2016). The payload capacity was increased by concealing the secret data into two-layers using a security system implemented by combining AES cryptography and image steganography (Al-otaibi and Gutub, 2014b). Li et al. (2015) had used the cross division and additive homomorphism to develop a new reversible data hiding scheme for encrypted image to enhance the privacy protection in multimedia applications. The homomorphic technique was adopted in their work due to the fact that it allows computation with encrypted data without causing their expansion which in turn improves the embedding capacity. To perform the embedding, the encryption key was utilized to encrypt the cover image, after that the data embedding key was applied to conceal data into the encrypted cover image. Besides, to make this scheme reversible, histogram shifting was also adopted. The extraction does not depend on the image decryption at the receiver side, i.e., the extraction of the embedded data can be performed before or after decrypting the encrypted image.

Chen et al. (2016) presented a method based on contrast enhancement, pixel value ordering and histogram shifting. An approach that categorizes pixels into different regions, i.e., smooth and complex regions so as to identify pixels that can hold the secret bits with less distortion of the stego image was suggested by Nguyen et al. (2016) and the extracted cover image and secret data are identical to those before the embedding process. Moreover, the performance of this approach was evaluated using encrypted images. Having the aim to increase both payload capacity and quality of the stego image, the DE and IRDE approaches presented by Alattar (2004) and Yi et al. (2009) were joined to build a reversible multilayer scheme in (Arham et al., 2017). The Zhang and Wang's EMD (Zhang and Wang, 2006) method gives more considerable cases which allows data to be easily embedded regardless of the ratio of the size of cover signal and the embedding capacity. Since the modification direction (MD) was completely exploited, high capacity was achieved. Xiao et al. (2017) proposed a new separable RDH for encrypted images that combined the homomorphism encryption and the pixel value ordering (PVO) techniques. Two keys (data hiding key and encryption key) were used. The data hiding key is used to recover the hidden additional data while the encrypted image is recovered using the encryption key which implies that to be able to recover all data, both keys have to be safely transmitted to the receiver. Employing the least significant bit (LSB) technique and the pixel indicator, Gutub et al. built a steganographic model that disguises sensitive data in RGB images (Gutub et al., 2010). Secret data were embedded in the reduced difference values (Ahmad et al., 2013; Maniriho and Ahmad, 2017).

Hong et al. (2012) developed an improved reversible DH Scheme by investigating each block's smoothness and employing the side-matching techniques to reduce the extracted-bits error rate. Their results reveal that the error rate was significantly decreased for all size of the pixel blocks. The LSB-matching approach that uses seven rules to disguise the modification of pixels was presented by Lu et al. (2015). Their approach employs the technique of dual image to embed confidential data. Dual image is one of the current reversible data hiding techniques which conceals data by creating two identical copies of the same original carrier image to be used for concealing data in order to increase the payload capacity. Their method proved this concept by yielding a high payload capacity while maintaining the quality of the stego image. The advances on the reversible data hiding (RDH) algorithms combined with applications domains were presented by Shi et al. (2016). Inspired by the concept of difference expansion, Abdullah and Manaf (2010) introduced a multilevel data hiding method based on DE. Horizontal and vertical scanning were performed to partition the cover image into non-overlapping blocks of size 2×1, after that the difference between pixels was calculated in each block and the embedding was performed based on some defined criteria. Firstly, the lookup table (LT) was used to record the position of all embedding pixel pairs. The LT is very useful during the embedding and data extraction. Secondly, all difference values were sorted to identify the smooth areas or blocks, i.e., any block where the difference is 0 or 1 was recorded as image smooth area and was utilized for embedding the secret data. Moreover, data were hidden in several layers so as to increase the capacity. However, even though a multilayer technique was applied, their method limits the embedding capacity since only two values are considered for embedding data. This limitation can be easily noticed in images with no smooth areas, which can greatly affect the embedding capacity.

Nevertheless, in the transform domain, the cover image is first converted form spatial to transform domain and the regions of the cover image that are less susceptible to image processing operations such as compression or copping are considered for concealing confidential information which results in high quality of the stego image (Li et al., 2011; Mehdi and Mureed, 2013). It should be noted that the modification is performed on the orthogonal transform of the image instated of the cover image itself. Fig. 2 presents some of the main techniques employed in the transform domain approach and the general block diagram illustrating the application of information hiding in the transform domain is provided in Fig. 3. JPEG image format is highly used in this domain. Techniques such as discrete wavelet transform and discrete cosine transform are less prone to malicious attacks (suspicion) particularly when the payload capacity is small, i.e., since only some coefficients in the transform domain are altered, the degradation of the image is not easily noticed. Usually, transform domain based methods achieve a low embedding capacity compared to the spatial domain based methods (Cheddad et al., 2010), however, their visual quality is relatively high.

To address the forgery encountered in medical images, Chiang et al. (2008) proposed two detection and restoration security system. The secret data were hidden in smooth blocks after dividing the image into blocks of size 4×4. Thereafter, the discrete wavelet transform (DWT) was applied to determine the smooth areas in the cover image. Additionally, the block was classified as smooth if all difference values are equals to zero and their scheme works well for medical images having smooth areas. The recovery of the secret data and the cover image do not require the embedding map. The disadvantage of this approach is that it does not perform well for medical images lacking smooth areas. Further details on the mod-

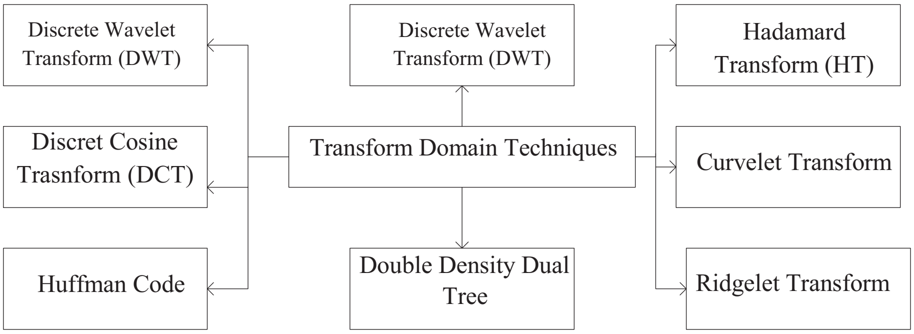

Discrete Wavelet Transform (DWT)
Discrete Wavelet Transform (DWT)
Hadamard Transform (HT)
Discret Cosine Trasnform (DCT)
Transform Domain Techniques
Curvelet Transform
Huffman Code
Double Density Dual Tree
Ridgelet Transform

Fig. 2. Techniques used in the transform domain approach.

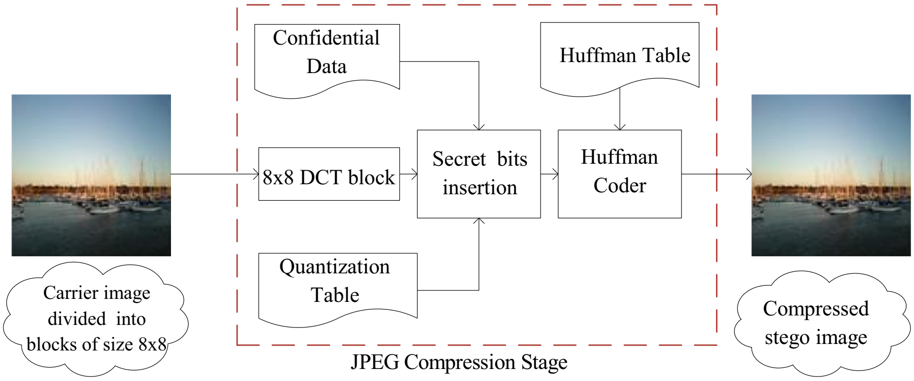


Fig. 3. General steps illustrating the embedding process in the transform domain (Qian and Zhang, 2012).

els based on the transform domain can be found in (Qian and Zhang, 2012), (Lin, 2014), (Wang et al., 2013), (Lin, 2012).

3. Proposed DE-based scheme

New information hiding methods are always needed to remove limitations or drawbacks encountered in the previous ones in order to increase their performance. In this direction, we propose a new data hiding method that is developed based on difference expansion (DE). The proposed method allows secret data to be hidden in both positive and negative difference calculated between pixels, which is different from Abdullah and Manaf's method (Abdullah and Manaf, 2010) that hides data in smooth areas, i.e. secret data were only hidden in values where the obtained difference is 1 or 0. Furthermore, their method has only considered positive values which may have a huge impact on the embedding capacity due to many values which are not utilized for embedding data. It can be inferred that such consideration can lead to a significant reduction of payload capacity for images where the presence of smooth areas is rare. Hence, the main goal of this method is to increase the embedding capacity while maintaining a good PSNR. In this way, two ranges that controls the embedding process are provided in order to ameliorate the performance. For the first range, we consider positive values which are between 0 and 2 ($0 \leqslant d \leqslant 2$) while for the second range negative values between -1 and -2 ($-1 \geqslant d \geqslant -2$) are considered. Note that d is used to denote the difference value.

To preserve the quality of the stego, the secret data are not concealed on the values which are out of both ranges. Some of the expressions for embedding, those are (1)–(3) are taken from the previous algorithm (Abdullah and Manaf, 2010). However, the extraction algorithms are totally different. Moreover, the modulus function is integrated in the proposed extraction algorithm to make the extraction process straightforward, i.e., it does remove complexity in recovering the concealed data. To demonstrate the functionality of this proposed scheme, the necessary steps required to conceal and extract the secret data are presented below. Moreover, Figs. 4–8, are also provided to illustrate the design and functionality of the proposed scheme.

3.1. Concealling the secret data

Similar to the other data hiding schemes, the embedding algorithm is one of the essential parts of this proposed method. Therein, the entire embedding process is accomplished throughout the following steps.

1. Segment the cover image into blocks of size 2×1
2. Calculate the difference between pixels in each block and store all values into an array (d_arr) using Eq. (1) where z and y denote the pair of pixel in each block while d represents the difference being computed.

$$d = z - y \tag{1}$$

3. Iterate through the array to get all values which satisfy the embedding conditions, i.e., identify all values that satisfy the first ($0 \leqslant d \leqslant 2$) and the second ($-1 \geqslant d \geqslant -2$) conditions (where these two conditions can be also simplified as $-2 \leqslant d \leqslant 2$), and disregard any difference value which is out of the range.
4. Utilize the tracing table (TRT), i.e., assign value in the TRT variable to distinguish all pairs as follows. If the first and second conditions are met, the bit 0 is assigned to the value of TRT variable whereas the bit 1 is used to identify those pairs which are unchanged (pairs having difference values which are out the range).

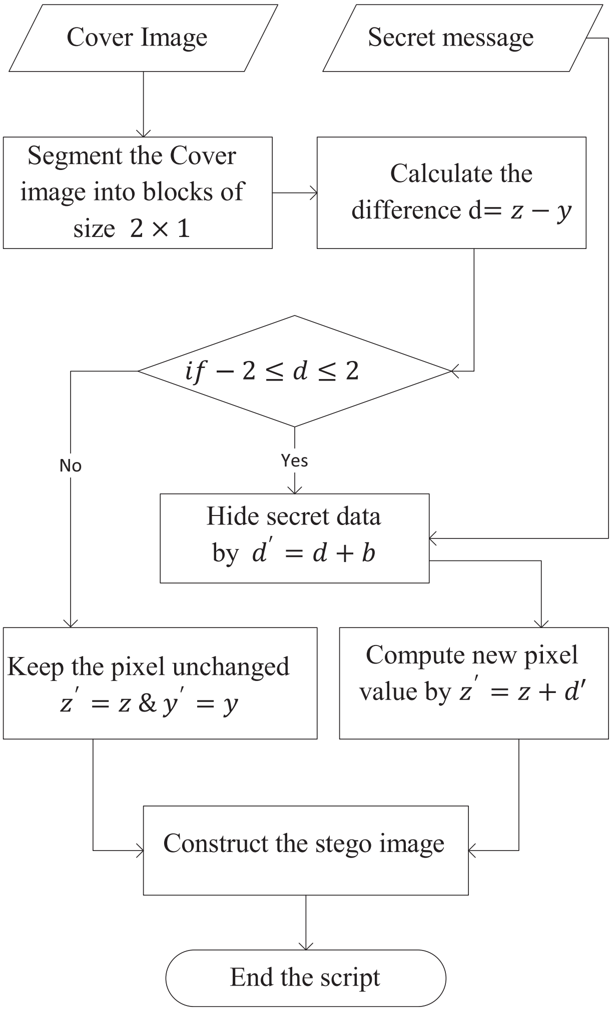

Cover Image
Secret message
Segment the Cover image into blocks of size 2 × 1
Calculate the difference d= z − y
if −2 ≤ d ≤ 2
No
Yes
Hide secret data by d′ = d + b
Keep the pixel unchanged z′ = z & y′ = y
Compute new pixel value by z′ = z + d′
Construct the stego image
End the script

Fig. 4. Embedding process for the proposed method.

5. Get the secret message and store it in a text file.
6. Based on the values obtained in the third step, hide the secret data by utilizing (2) to get the modified difference (d'), where b represents the secret bit to be hidden which can be zero or one, $b \to \{0,1\}$.

$$d' = d + b \tag{2}$$

7. Compute new pixel (z') having the secret bits using (3). Note that the new pixels are further used to construct the stego image.

$$z' = d' + z \tag{3}$$

As per the defined conditions for embedding data, below we present different scenarios that demonstrate how the secret data are concealed in the cover image.

1) *Scenario 1:* Difference $d \to 0$ and $b = 1$
Having a pair of pixels $z = 180,\ y = 180$ and the secret bits $b \to \{0,1\}$, the difference is first computed using (1) as shown in (4).

$$d = 180 - 180 = 0, \quad \text{and } TRT = 0 \tag{4}$$

The *TRT* value takes the bit zero (0) since the difference falls in the range. Notice that the TRT will be used later for extracting the hidden secret bits. After getting the difference, data can be hidden using (2) and the new pixel is computed using (3) whose computations can be seen in (5) and (6).

$$d' = 0 + 1 = 1 \tag{5}$$

$$z' = 180 + 1 = 181 \tag{6}$$

2) *Scenario 2: Difference* $d \to 1$ and $b = 1$ with $z = 181$ and $y = 180$ (For the next scenarios the same procedures in (4)–(6) are applied).

$$d = 181 - 180 = 1, \quad \text{and } TRT = 0 \tag{7}$$

$$d' = 1 + 1 = 2 \tag{8}$$

$$z' = 181 + 2 = 183 \tag{9}$$

3) *Scenario 3: Difference* $d \to 2$ and $b = 1$ with $z = 182$ and $y = 180$,

$$d = 182 - 180 = 2, \quad \text{and } TRT = 0 \tag{10}$$

$$d' = 2 + 1 = 3 \tag{11}$$

$$z' = 182 + 3 = 185 \tag{12}$$

4) *Scenario 4:* Difference $d \to -1$ and $b = 1$ with $z = 180$, and $y = 181$

$$d = 180 - 181 = -1, \quad \text{and } TRT = 0 \tag{13}$$

$$d' = -1 + 1 = 0 \tag{14}$$

$$z' = 180 + 0 = 180 \tag{15}$$

5) *Scenario 5: Difference* $d \to -2$ and $b = 0$ with $z = 180$ *and* $y = 182$,

$$d = 180 - 182 = -2, \quad \text{and } TRT = 0 \tag{16}$$

$$d' = -2 + 0 = -2 \tag{17}$$

$$z' = 180 - 2 = 178 \tag{18}$$

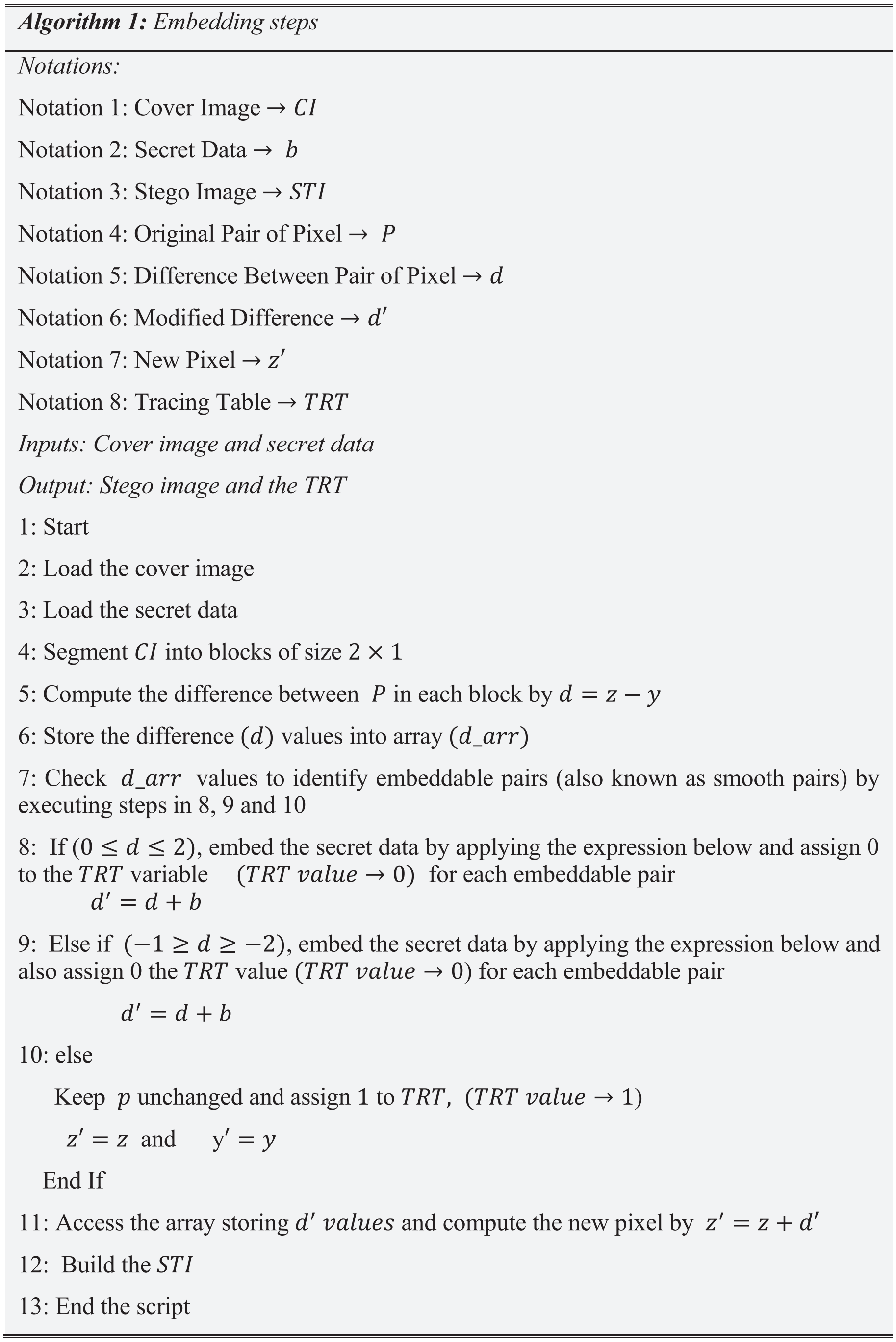
6) *Scenario 6: Difference* $d \to -2$ and $b = 1$ withz $= 102$ *and* $y = 104$

$$d = 102 - 104 = -2, \quad \text{and } TRT = 0 \tag{19}$$

$$d' = -2 + 1 = -1 \tag{20}$$

$$z' = 102 - 1 = 101 \tag{21}$$

For scenarios 2, 3, 4, 5 and 6, the TRT is also taking the value of 0 since the difference values fall in the proposed range. After hiding data, the new pixel pairs become, 1st pair $(z = 180,\ y = 180) \to (z' = 181,\ y' = 180)$, 2nd pair$(z = 181,\ y = 180) \to (z' = 183,\ y' = 180)$, 3rd pair$(z = 182,\ y = 180) \to (z' = 185,\ y' = 180)$, 4th pair$(z = 180,\ y = 181) \to (z' = 180,\ y' = 181)$, 5th pair $(z = 180,\ y = 182) \to (z' = 178,\ y' = 182)$ and 6th pair $(z = 102,\ y = 104) \to (z' = 101,\ y' = 104)$ with the secret bits $b \to \{111101\}$. Additionally, to keep pixels in the gray level range the new pixel value must be between 0 and 255 (new pixel $\to 0 \leqslant new\ pixel \leqslant 255$). This allows the hidden data and the cover image to be recovered without any distortions. The tracing table and the stego image are transmitted separately as concatenating them may decrease the quality of the stego image which can lead to its suspicion and unauthorized data access. Therein, they are kept separate.



```
Algorithm 1: Embedding steps
Notations:
Notation 1: Cover Image → $CI$
Notation 2: Secret Data → $b$
Notation 3: Stego Image → $STI$
Notation 4: Original Pair of Pixel → $P$
Notation 5: Difference Between Pair of Pixel → $d$
Notation 6: Modified Difference → $d'$
Notation 7: New Pixel → $z'$
Notation 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: Compute the difference between $P$ in each block by $d = z - y$
6: Store the difference $(d)$ values into array $(d\_arr)$
7: Check $d\_arr$ values to identify embeddable pairs (also known as smooth pairs) by
   executing steps in 8, 9 and 10
8: If $(0 \leq d \leq 2)$, embed the secret data by applying the expression below and assign 0
   to the $TRT$ variable $(TRT\ value \rightarrow 0)$ for each embeddable pair
        $d' = d + b$
9: Else if $(-1 \geq d \geq -2)$, embed the secret data by applying the expression below and
   also assign 0 the $TRT$ value $(TRT\ value \rightarrow 0)$ for each embeddable pair
        $d' = d + b$
10: else
     Keep $p$ unchanged and assign 1 to $TRT$, $(TRT\ value \rightarrow 1)$
      $z' = z$ and $y' = y$
   End If
11: Access the array storing $d'\ values$ and compute the new pixel by $z' = z + d'$
12: Build the $STI$
13: End the script
```

Fig. 5. Algorithm for concealing secret data.

3.2. Recovering the concealed secret data

The extraction of the hidden data is performed using the tracing table defined during the embedding process. Similar to the embedding, the stego image is first segmented into blocks of the same size (2 by 1), thereafter the difference between each pixel's pair is computed using the equation in (22). Once all differences values have been obtained, the hidden secret data are extracted using the modulus function and the *TRT* (23). Besides, since the cover image has to be reconstructed, the first part of the expression in (24) is given to recover the original pixel's value when the *TRT* value is 0 otherwise as it is shown in the second part of (24), the original pixel's value is equivalent to the stego pixel. Additionally, Fig. 6 illustrates how both embedding and extraction processes are performed given the cover image and confidential (secret) data to be concealed, while Figs. 7 and 8 present the design and the steps for the extraction algorithm.

$$d'' = z' - y' \tag{22}$$

$$b = d''\ mod\ 2 \quad if\ TRT = 0 \tag{23}$$

$$\begin{cases} z = z' - \left\lceil \frac{z' - y'}{2} \right\rceil & if\ TRT = 0 \\ z = z', & otherwise \end{cases} \tag{24}$$

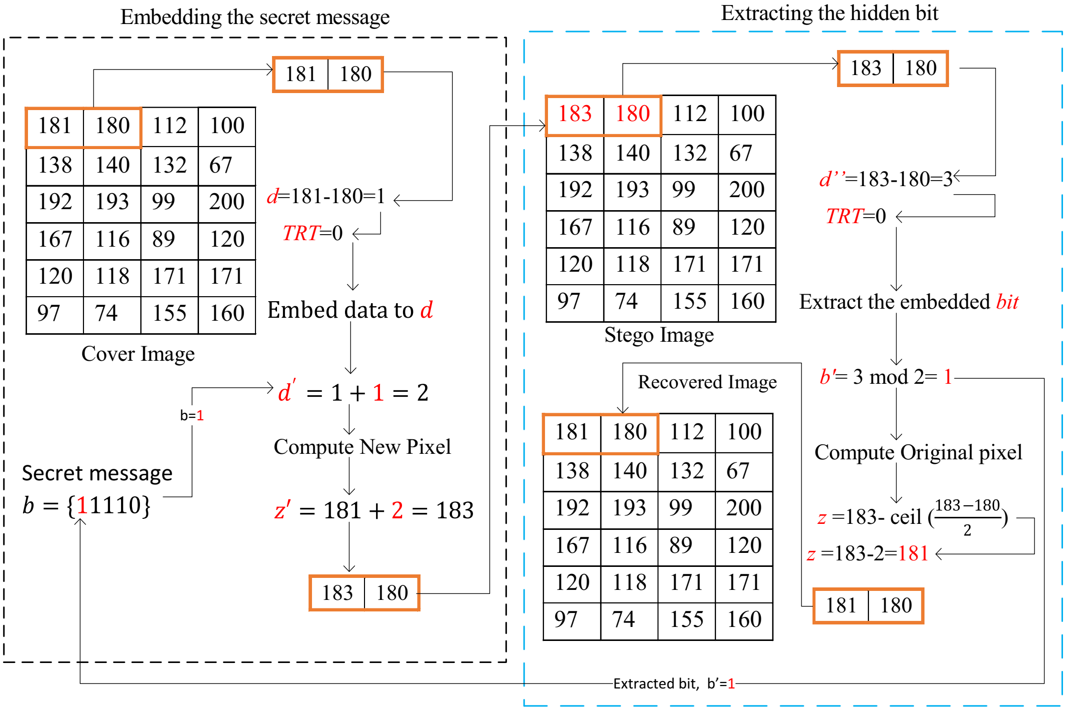


Fig. 6. A block diagram demonstrating concealment and extraction stages using the proposed method.

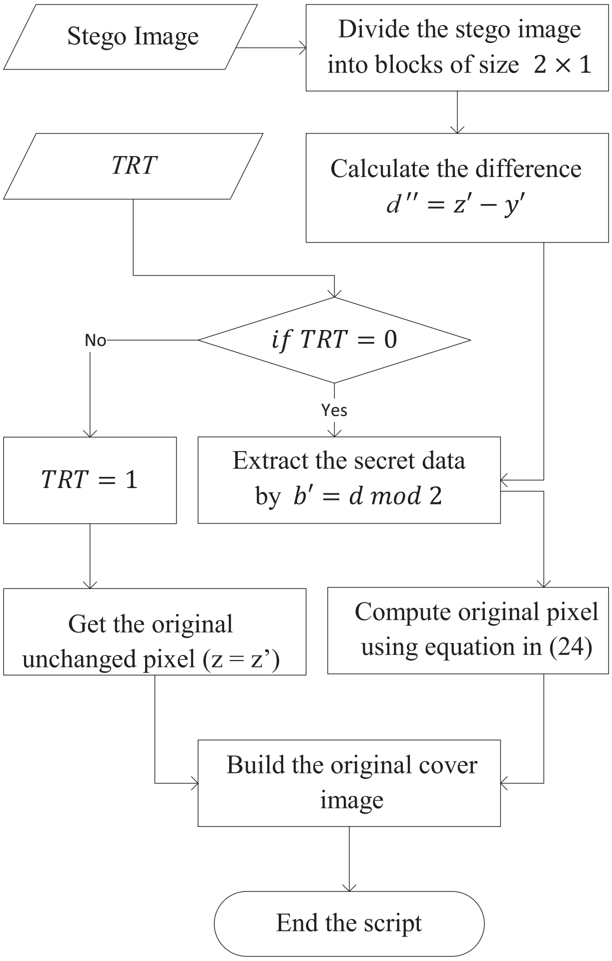

Stego Image
Divide the stego image into blocks of size 2 × 1
TRT
Calculate the difference d″ = z′ − y′
if TRT = 0
No
Yes
TRT = 1
Extract the secret data by b′ = d mod 2
Get the original unchanged pixel (z = z’)
Compute original pixel using equation in (24)
Build the original cover image
End the script

Fig. 7. Extracting the concealed secret data.

In this way, considering the previous stego pixels, the hidden data and the original pixels can be recovered by applying equations in (22)–(24) as it is performed from the first scenario till the last one (the sixth scenario) where these scenarios are the reverse of the ones executed during the embedding process. Furthermore, as shown below, the same steps in (25)–(27) are also applied for other pairs (from scenario 2 till 6). Schematic representation for the embedding and extraction steps can be viewed in Fig. 6.

1) *Recovery scenario 1: First pair of pixel* → $(z' = 181,\ y' = 180)$

$$d'' = 181 - 180 = 1 \tag{25}$$

$$\rightarrow TRT = 0$$

$$b' = d''\ mod\ 2 = 1\ mod\ 2 = 1 \tag{26}$$

$$z = 181 - \left\lceil \frac{181 - 180}{2} \right\rceil = 181 - \left\lceil \frac{1}{2} \right\rceil \tag{27}$$

$$z = 181 - \lceil 0.5 \rceil = 180$$

2) *Recovery scenario 2: Second pair of pixel* → $(z' = 183,\ y' = 180)$

$$d'' = 183 - 180 = 3 \tag{28}$$

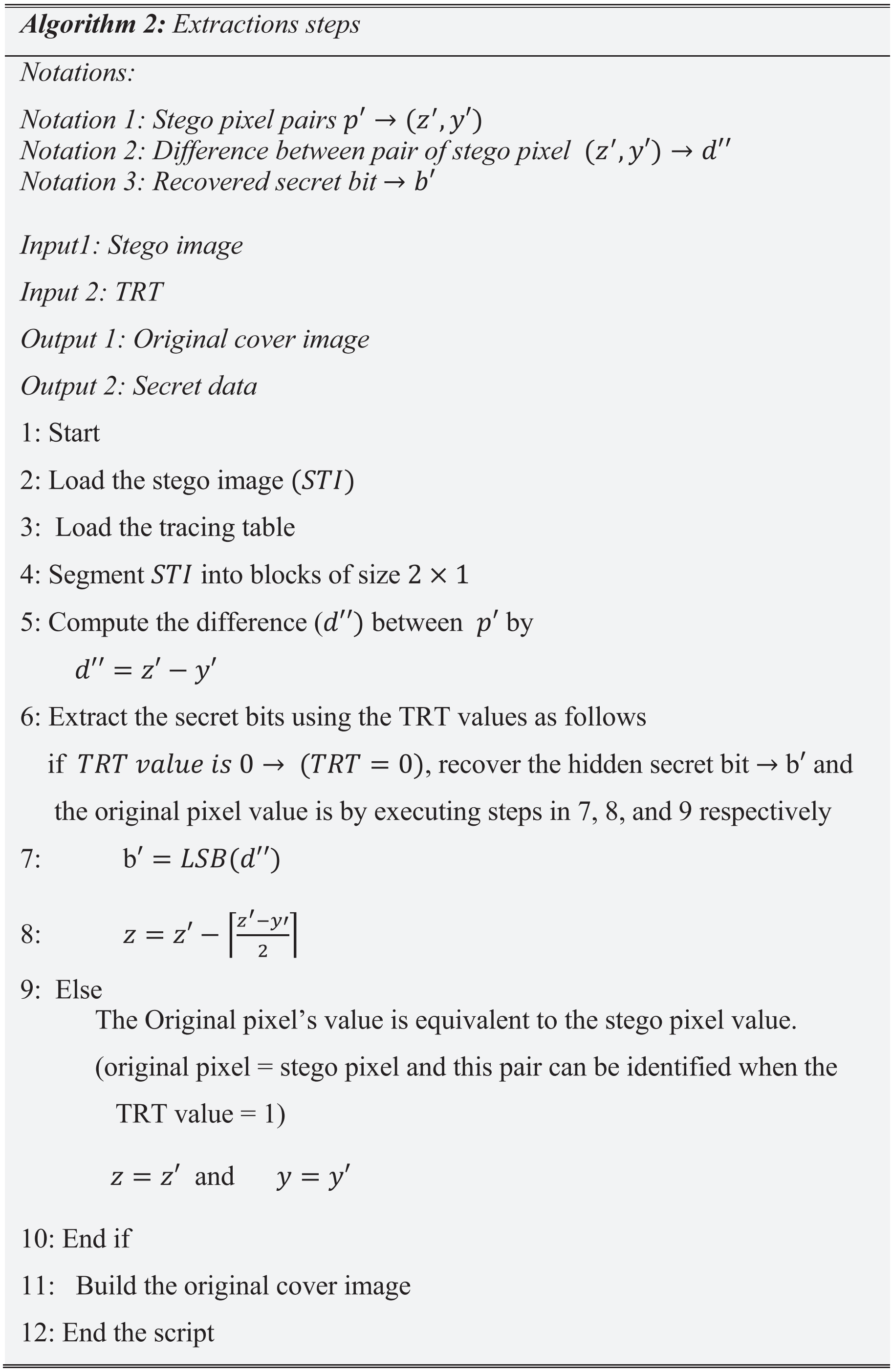
$$\rightarrow TRT = 0$$

$$b' = d''\ mod\ 2 = 3\ mod\ 2 = 1 \tag{29}$$

$$z = 183 - \left\lceil \frac{183 - 180}{2} \right\rceil = 183 - \left\lceil \frac{3}{2} \right\rceil = 183 - 2 = 181 \tag{30}$$

3) *Recovery scenario 3: Third pair of pixel* → $(z' = 185,\ y' = 180)$

$$d'' = 185 - 180 = 5 \tag{31}$$



```
Algorithm 2: Extractions steps
Notations:
Notation 1: Stego pixel pairs $p' \rightarrow (z', y')$
Notation 2: Difference between pair of stego pixel $(z', y') \rightarrow d''$
Notation 3: Recovered secret bit $\rightarrow b'$

Input1: Stego image
Input 2: TRT
Output 1: Original cover image
Output 2: Secret data
1: Start
2: Load the stego image ($STI$)
3:  Load the tracing table
4: Segment $STI$ into blocks of size $2 \times 1$
5: Compute the difference ($d''$) between $p'$ by
       $d'' = z' - y'$
6: Extract the secret bits using the TRT values as follows
     if $TRT\ value\ is\ 0 \rightarrow (TRT = 0)$, recover the hidden secret bit → $b'$ and
     the original pixel value is by executing steps in 7, 8, and 9 respectively
7:          $b' = LSB(d'')$
8:          $z = z' - \left\lceil \frac{z'-y\prime}{2} \right\rceil$
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)
         $z = z'$  and      $y = y'$
10: End if
11:   Build the original cover image
12: End the script
```

Fig. 8. Algorithm for extracting the hidden data.

$\rightarrow TRT = 0$

$$b' = d''\ mod\ 2 = 5\ mod\ 2 = 1 \tag{32}$$

$$z = 185 - \left\lceil \frac{185-180}{2} \right\rceil = 183 - \left\lceil \frac{5}{2} \right\rceil = 185 - 3 = 182 \tag{33}$$

4) *Recovery scenario 4: Fourth pair of pixel* $\rightarrow (z' = 180,\ y' = 181)$

$$d'' = 180 - 181 = -1 \tag{34}$$

$\rightarrow TRT = 0$

$$b' = d''\ mod\ 2 = abs(-1)\ mod\ 2 = 1 \tag{35}$$

$$z = 180 - \left\lceil \frac{180-181}{2} \right\rceil = 180 - \left\lceil \frac{-1}{2} \right\rceil = 180 - -\lceil 0.5 \rceil = 180 - 0 = 180 \tag{36}$$

5) *Recovery scenario 5: fifth pair of pixel* $\rightarrow (z' = 178,\ y' = 182)$

$$d'' = 178 - 182 = -4 \tag{37}$$

$\rightarrow TRT = 0$

$$b' = d'' \ mod \ 2 = abs(-4) \ mod \ 2 = 0 \tag{38}$$

$$\begin{aligned} z &= 178 - \left\lceil \frac{178-182}{2} \right\rceil = 178 - \left\lceil \frac{-4}{2} \right\rceil \\ &= 178 - -\lceil 2 \rceil = 180 \\ &= 178 + 2 = 180 \end{aligned} \tag{39}$$

6) *Recovery scenario 6: Sixth pair of pixel* → $(z' = 101, \ y' = 104)$

$$d'' = 101 - 104 = -3 \tag{40}$$

$$\rightarrow TRT = 0$$

$$b' = d'' \ mod \ 2 = abs(-3) \ mod \ 2 = 1 \tag{41}$$

$$\begin{aligned} z &= 101 - \left\lceil \frac{101-104}{2} \right\rceil = 101 - \left\lceil \frac{-3}{2} \right\rceil \\ &= 101 - -\lceil 1.5 \rceil \\ &= 101 + 1 = 102 \end{aligned} \tag{42}$$

The ceiling brackets $\lceil z \rceil$ allow the value of z to be rounded to the nearest integer greater than or equal to z while the floor brackets $\lfloor z \rfloor$ round the value of z to the nearest integer less than or equal to z. The extracted secret bits in (26), (29), (32), (35), (38) and (41), $b \rightarrow \{111101\}$ and the values of the recovered pixels in (27), (30), (33), (36), (39) and (42) are exactly the same as the original ones. Therefore, based on the above operations, the reversibility of the proposed method can be easily seen. That is, the hidden secret data and the original cover image can be recovered without any dissimilarities or deformations.

4. Results and discussion

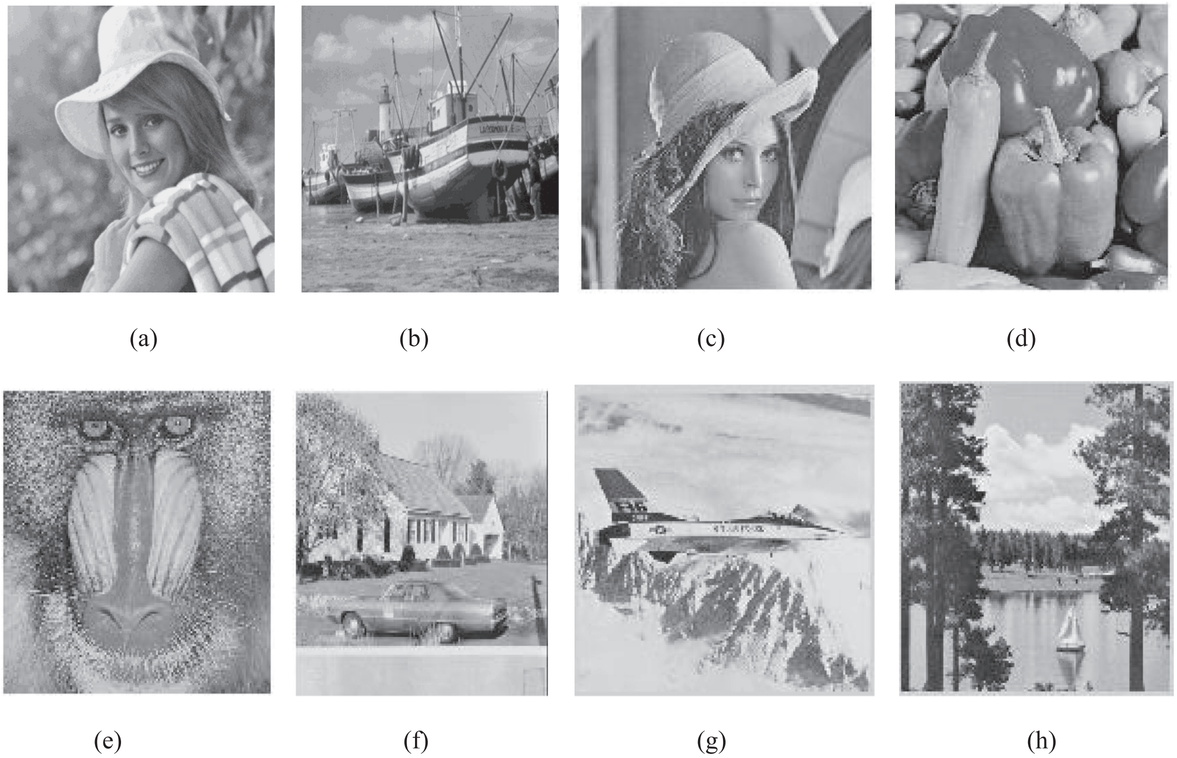
In this section, we present the results from the experiment. The peak signal to noise ratio (PSNR) and the embedding capacity are measured in order to assess the performance of the suggested scheme. To compute the PSNR, (43) is used while (44) is used for computing the mean squared error (MSE). In (44), $CI(i,j)$ is used to indicate the ith pixel in the cover image CI whereas $STI(i', \ j')$ represents the ith pixel in the stego image STI.

$$PSNR = 10\log_{10}\frac{(255)^2}{\text{MSE}} \tag{43}$$

$$MSE = \frac{1}{(G \times H)}\sum_{i=1}^{G}\sum_{j=1}^{H}[CI(i,j) - STI(i',j')]^2 \tag{44}$$

The PSNR is measured in order to analyze the dissimilarities between the cover image and stego image after concealing data. This makes sense since any drastic distortion that occurs in the stego image may lead to the unauthorized access. Hence, the PSNR value helps to assess the distortion very easily. The embedding capacity is the number of secret bits that can be concealed in the cover image.

The test images used during the evaluation are given in Fig. 9 while Figs. 10 and 11 shows the gap between the capacities for both methods. Overall, the experimental results are presented as follows. Table 1 presents the total number of possible embeddable pairs which are identified in each cover image based on the values obtained after computing the difference between pixel pairs. It is also worth to mention that these are the pairs that generate difference values which fall into the defined ranges and they are said to be smooth pairs due to their characteristics of preventing changes


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

(e) (f) (g) (h)

Fig. 9. Original test images taken from (Califonia UUo, 2017) (a) Elaine.tiff (b) Boat.tiff (c) Lena.tiff (d) Girl.tiff (d) Pepper.tiff (e) Baboon.tiff (f) House.tiff (g) Aeroplane.tiff (h) Trees.tiff.

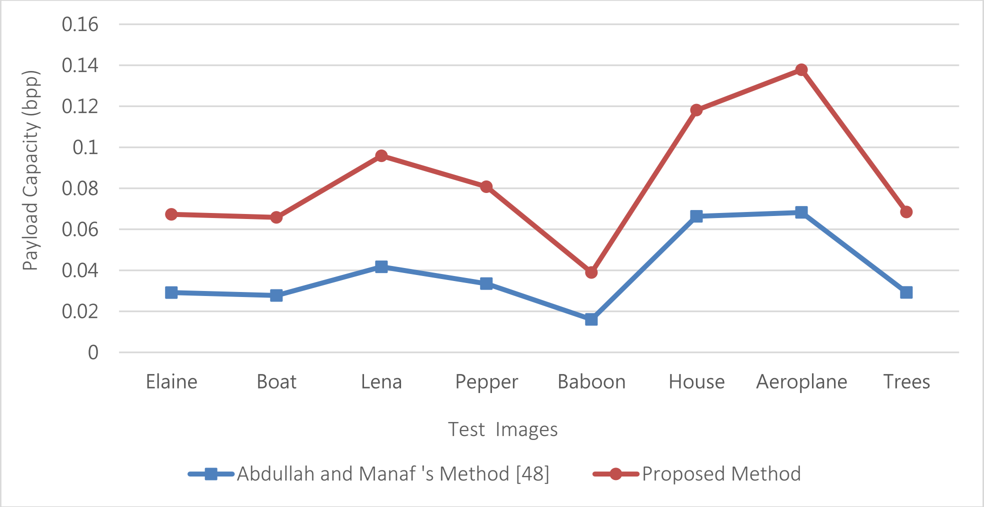


Fig. 10. Payload capacity (in bpp) for Abdullah and Manaf's method (Abdullah and Manaf, 2010) and the proposed one after concealing data.

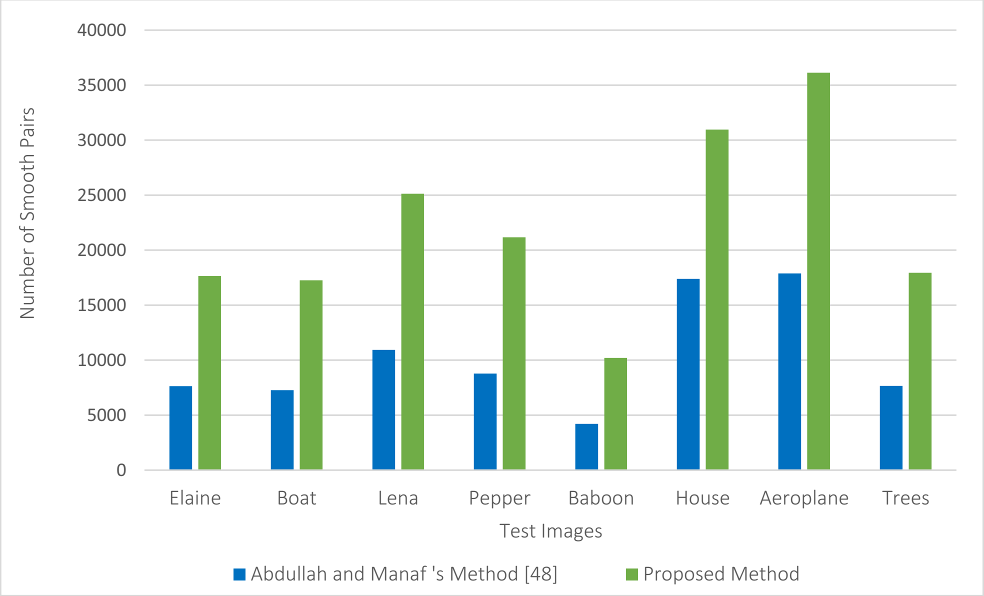


Fig. 11. Maximum number of smooth pairs per image using Abdullah and Manaf (Abdullah and Manaf, 2010) and the proposed method.

from being easily noticed after concealing secret data. Furthermore, the capacity in bit per pixel (bpp) which is computed by taking the total number of bits that can be held by the cover image divided by its dimension, and the PSNR values are also provided.

Since images possess different properties such as edges, they also hide different capacities. That is, the number of bits to be concealed highly depends upon the nature of the cover image itself. This implies that for those images having several smooth pairs, the capacity will be high while if they possess few smooth areas, the capacity will not be high. The example can be seen from Table 1 where cover images like Lena (0.0958 bpp), House (0.1181 bpp) and Aeroplane (0.1378 bpp) are holding a large number of bits compared to the other images. Few smooth pairs are found in Baboon (10,208 pairs) which results in low payload capacity (0.0389 bpp). In general, it is shown that the number of smooth pairs is proportional to the number of bits which can be embedded into the cover image. Furthermore, the PSNR value is slightly decreased compared to the previous method due to the capacity which is significantly increased more than twice for all cover images. However, the PSNR for the proposed method is still good since if the PSNR is greater than 30 dB, the cover image and the stego image similarity is generally high which results in protecting the hidden confidential data from being tampered or accessed by unintended recipients (Tang et al., 2014).

Fig. 12 is provided to illustrate the example of the cover image histogram before and after hiding data. The concept of using histogram to visualize the changes made in the image was discussed in the work presented by Fridrich et al. (2003) which reveals that significant changes in the cover image's histogram can lead to the stego image suspicion which can results in intercepting or interfering the hidden data. Hence, drastic changes in the histogram of the stego image are always undesirable while concealing data in any media. The example of the stego image histogram can be viewed from Fig. 12 where (a) and (b) depict both histograms of Trees.tiff cover image before and after concealing the payload capacity of size 0.0684 bpp. If we look at the image histogram in

Table 1
Payload Capacity, PSNR and computational Time Obtained after Concealing Data.

Cover Images	(Abdullah and Manaf, 2010)				Proposed Method			
	Total number of smooth pairs	Embedding capacity (bpp)	PSNR (dB)	Computational time (second)	Total number of smooth pairs	Embedding Capacity (bpp)	PSNR (dB)	Computational time (second)
Elaine	7637	0.0291	61.994	3.818	17,645	0.0673	56.2007	3.738
Boat	7271	0.0277	62.0754	3.643	17,255	0.0658	56.1899	3.122
Lena	10,937	0.0417	60.3041	3.607	25,124	0.0958	54.5336	3.721
Pepper	8784	0.0335	61.1104	3.377	21,171	0.0807	55.1808	3.622
Baboon	4210	0.0160	64.1743	3.905	10,208	0.0389	58.2953	3.726
House	17,387	0.0663	58.7591	3.871	30,960	0.1181	54.593	3.656
Aeroplane	17,883	0.0682	58.3034	3.650	36,127	0.1378	53.478	3.839
Trees	7659	0.0292	61.8376	3.567	17,949	0.0684	56.0315	3.718

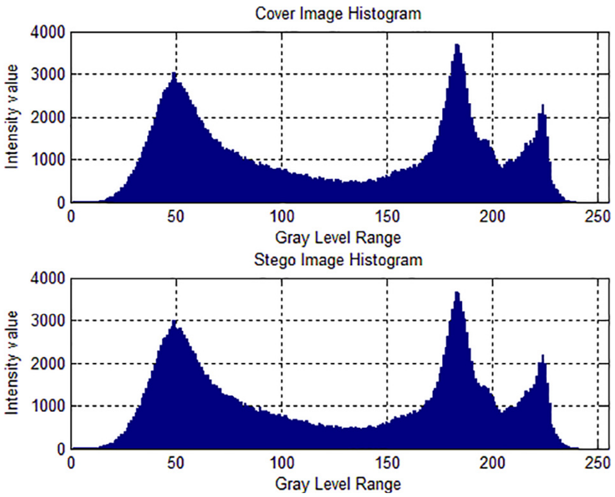


Fig. 12. Trees cover image.tiff (a) Histogram before hiding data with image pixels' average = 125.2349 (b) Histogram after hiding payload capacity of size 0.0684 bpp, with image pixels' average = 125.2683 and PSNR = 56.0316 decibels (dB).

(a) and (b) they are almost similar which makes the proposed method to be highly judged invisible. Moreover, considering the pixels' average for both images, cover image pixels' average = 125.2349 and stego image pixels' average = 125.2683, they tend to be close to each other which proves their high degree of resemblance. Moreover, as presented in Table 1 the computational time for these algorithms is also evaluated where the proposed method has a lower average computational time which is 3.642 s over 3.679 s from Abdullah and Manaf's method, i.e., the proposed method is 0.037 s faster.

Furthermore, Tables 2 and 3 present the comparison between the proposed DE based method and the previous ones in terms of the visual quality of the stego image and computational time. The first comparison is made between Alattar's work (Alattar, 2004) while the second one is made between Ahmad et al.'s method (Ahmad et al., 2013). From both tables it could be seen that the proposed method achieves good PSNR over both methods. Taking into account the computational time, Alattar's work has the lowest average computational time of (2.414 s). That is, Alattar's method (Alattar, 2004) is 1.228 faster than the proposed method. Nevertheless, Ahmad et al.'s method (Ahmad et al., 2013) average computational time (4.3184 s) is higher than the one from the proposed method (3.642) which makes it to be 0.6764 s slower than the proposed method. It is crucial to mention that the computational time also depends on the nature of the image and that is why different execution times are obtained for all cover images. From Table 1 after applying the proposed method the highest execution time (3.738) is obtained while concealing confidential data

Table 2
Comparison between (Alattar, 2004) and the proposed method in terms of quality of the stego image (PSNR) and computational time.

Cover Images	(Alattar, 2004)			Proposed Method		
	Capacity in bit per pixel (bpp)	PSNR (dB)	Computational time (second)	Capacity in bit per pixel (bpp)	PSNR (dB)	Computational time (second)
Elaine	0.0673	53.6051	2.226	0.0673	56.2007	3.738
Boat	0.0658	53.8217	2.169	0.0658	56.1899	3.122
Lena	0.0958	49.6814	2.421	0.0958	54.5336	3.721
Pepper	0.0807	51.8896	2.427	0.0807	55.1808	3.622
House	0.1181	53.9278	2.701	0.1181	54.593	3.656
Aeroplane	0.1378	47.8339	2.767	0.1378	53.478	3.839
Trees	0.0684	54.4153	2.189	0.0684	56.0315	3.718

Table 3
Comparison between (Ahmad et al., 2013) and the proposed method in terms of quality of the stego image and computational time.

Cover Images	(Ahmad et al., 2013)			Proposed Method		
	Capacity in bit per pixel (bpp)	PSNR (dB)	Computational time (second)	Capacity in bit per pixel (bpp)	PSNR (dB)	Computational time (second)
Elaine	0.0673	45.3769	7.006	0.0673	56.2007	3.738
Boat	0.0658	45.6966	3.760	0.0658	56.1899	3.122
Lena	0.0958	46.7301	4.890	0.0958	54.5336	3.721
Pepper	0.0807	41.1211	3.927	0.0807	55.1808	3.622
House	0.1181	41.5015	3.813	0.1181	54.593	3.656
Aeroplane	0.1378	43.2581	3.587	0.1378	53.478	3.839
Trees	0.0684	40.6923	3.246	0.0684	56.0315	3.718

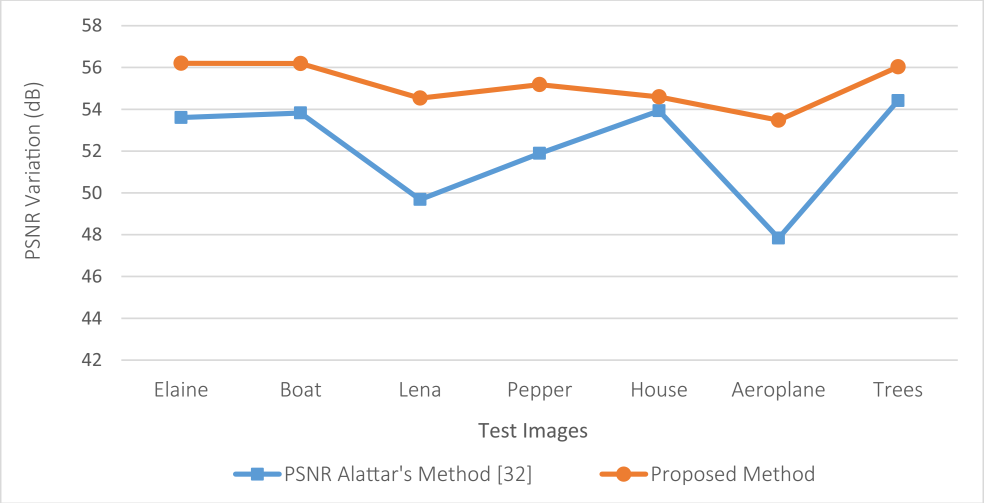


Fig. 13. Comparison in terms of PSNR variation between Alattar's method (Alattar, 2004) and the proposed one.

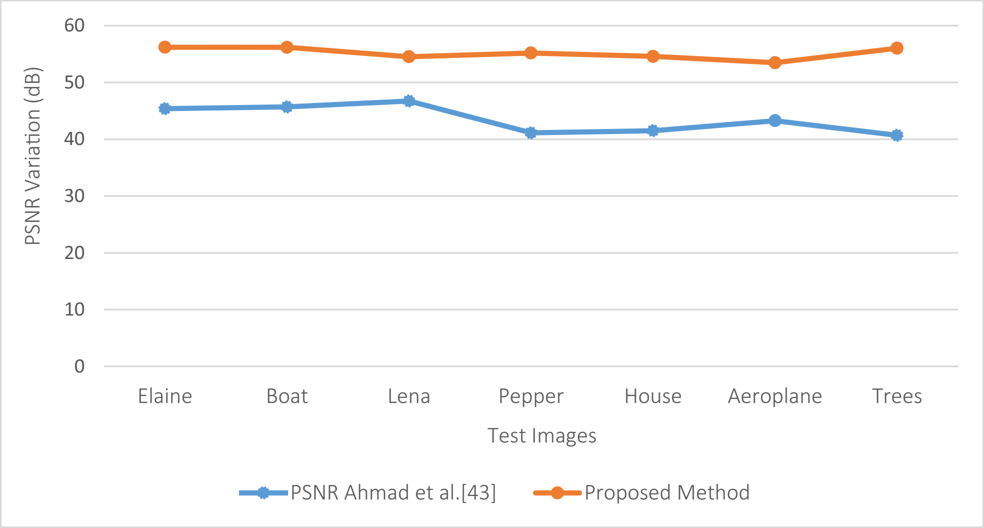


Fig. 14. Comparison in terms of PSNR variation between Ahmad et al.'s method (Ahmad et al., 2013) and the proposed one.

(0.0673 bpp) in Elaine.tiff cover image whereas the lowest execution time (3.122 s) is achieved in Boat.tiff cover image after concealing the payload capacity of size 0.0658 bpp. The results presented in Tables 2 and 3 are visualized in Fig. 13 and Fig. 14. Consequently, regarding the number of embeddable pairs not all values are falling in the defined ranges after computing the difference in each block which can results in slightly decreasing the embedding capacity in case several pairs are not utilized for concealing confidential data. In general, the proposed approach can be highly applicable in situations where small or medium embedding capacity is required.

5. Conclusion

Several information hiding methods that protect confidential data by concealing them into the other multimedia objects have been developed in the recent years. The embedding capacity and the similarity between the cover image and its respective stego image are among the major concerns to be highly considered while developing information hiding method. Besides, difference expansion is one the most popular reversible data hiding schemes due to its ability of reversibly recovering the hidden data and the original cover image without degradations. This advantage provided by DE-based schemes is often exploited in situations such as satellite and medical images to provide authentication, user privacy, content and copyright protection where the similar cover image must be reconstructed after extracting the hidden confidential data. Thereby, to also exploit this advantage, an improvement of the existing DE-based scheme is presented in this paper, i.e., an improved reversible data hiding scheme based on difference expansion and modulus function that allows the secret data to be concealed into digital images is developed. Confidential data are concealed into the difference computed between pixel pairs in each block.

Furthermore, two ranges are defined to determine the appropriate embeddable pixel pairs (also known as smooth pairs) which achieves good embedding capacity. The tracing table defined during the embedding and the modulus function are used to extract the hidden data and to reconstruct the original cover image. Factors such as computational time are also taken into account during the performance evaluation. The proposed DE provides a high capacity over the previous DE-based method while maintaining a high similarity between the cover and the stego image which thoroughly demonstrates its performance. However, as presented in experimental results' discussion, further improvements on the embedding capacity and execution time are still needed in the future work.

Acknowledgment

This research is supported by the Ministry of Research, Technology and Higher Education, Republic of Indonesia.

References

Abdullah, S.M., Manaf, A.A., 2010. In: Multiple Layer Reversible Images Watermarking Using Enhancement of Difference Expansion Techniques. Springer-Verlag Berlin Heidelb., pp. 333–342.

Ahmad, T., Holil, M., Wibisono, W., Royyana Muslim, I., 2013. An improved Quad and RDE-based medical data hiding method. In: International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM), pp. 141–145.

Alattar, A.M., 2004. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image Process. 13 (8), 1147–1156.

Alattar, A.M., 2004. Reversible watermark using difference expansion of quads Proceedings (ICASSP '04), no. 1. In: IEEE Int. Conf. Acoust. Speech, Signal Process, pp. 377–380.

Al-otaibi, N.A., Gutub, A.A., 2014b. 2-Leyer security system for hiding sensitive text data on personal computers. In: Lect. Notes Inf. Theory, pp. 151–157. April 2017.

Al-otaibi, N.A., Gutub, A.A., 2014a. Flexible stego-system for hiding text in images of personal computers based on user security priority. In: (AET-2014), Proceedings of 2014 International conference on Advanced Engineering Technologies, pp. 250–256.

Al-qershi, O.M.M., Khoo, B.E., 2011. High capacity data hiding schemes for medical images based on difference expansion. J. Syst. Softw. 84 (1), 105–112.

Andra, M.B., Ahmad, T., Usagawa, T., 2017. Medical record protection with improved GRDE data hiding method on audio files. Eng. Lett. 25 (2), 112–124.

Arham, A., Nugroho, H.A., Adji, T.B., Grafika, J., Campus, N., 2016. Combination schemes reversible data hiding for medical images. pp. 2–7.

Arham, A., Nugroho, H.A., Adji, T.B., 2017. Multiple layer data hiding scheme based on difference expansion of quad. Signal Process. 137, 52–62.

Bugár, G., Bánoci, V., Broda, M., Levický, D., Dupák, D., 2014. Data hiding in still images based on blind algorithm of steganography 2, pp. 8–11.

Califonia UUo, &quot;SIPI Image Database,&quot; [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc. (accessed: 22.03.2017).

Cheddad, A., Condell, J., Curran, K., Kevitt, P.M., 2008. Enhancing steganography in digital images. In: Canadian Conference on Computer and Robot Vision, pp. 326–332.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P., 2010. Digital image steganography: survey and analysis of current methods. Signal Process. 90 (3), 727–752.

Chen, H., Ni, J., Hong, W., Chen, T., 2016. Reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering. Signal Process. Image Commun. 46, 1–16.

Chiang, K.H., Chang-Chien, K.C., Chang, R.F., Yen, H.Y., 2008. Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. J. Digit. Imaging 21 (1), 77–90.

El-sayed, H.S., El-zoghdy, S.F., Faragallah, O.S., 2016. Adaptive difference expansion-based reversible data hiding scheme for digital images. Arab. J. Sci. Eng. 41 (3), 1091–1107.

Firmansyah, D.M., Ahmad, T., 2016. An improved neighbouring similarity method for video steganography. International Conference on Cyber and IT Service Management.

Fridrich, J., Goljan, M., Hogea, D., 2003. New methodology for breaking steganographic techniques for JPEGs. Proc. SPIE 5020, 143–155.

Gutub, A., Ankeer, M., Abu-ghalioun, M., Shaheen, A., Alvi, A., 2010. Pixel indicator high capacity technique for Rgb image based steganography. J. Emerg. Technol. Web Intell. 2 (1), 56–64.

Gutub, A., Al-Juaid, N., Khan, E., 2017. Counting-based secret sharing technique for multimedia applications. Springer, Multimed Tools Appl.

Han, D., Yang, J., Summers, W., 2017. Inject stenography into cybersecurity education. In: 2017 31st International Conference on Advanced Information Networking and Applications Workshops Inject, pp. 50–55.

Hong, W., Chen, T., Wu, H., 2012. An improved reversible data hiding in encrypted images using side match 19(4), 199–202.

Kaur, S., Goel, N., 2015. Segmentation and block based image steganography using optimal pixel adjustment process and identical approach. In: Proc. 2015 RAECS VIET Panjab Univ. Chandigarh 21-22nd December 2015 Segmentation, pp. 1–5.

Khandelwal, P., Bisht, N., Thanikaiselvan, V., 2015. Randomly hiding secret data using dynamic programming for image steganography. In: EEE International Conference on Computing and Network Communications (CoCoNet'15), pp. 777–783.

Li, B., Junhui, H., Jiwu, H., Yun, Q.S., 2011. A survey on image steganography and steganalysis. J. Inf. Hiding Multimed. Signal Process. 2 (2), 142–172.

Li, Q., Liao, X., Chen, G., Ding, L., 2017. A novel game-theoretic model for content-adaptive image steganography. In: 2017 IEEE 37th Int. Conf. Distrib. Comput. Syst. Work. A, pp. 232–237.

Li, M., Xiao, D., Zhang, Y., Nan, H., 2015. Reversible data hiding in encrypted images using cross division and additive homomorphism. Signal Process. Image Commun. 39, 234–248.

Lin, Y., 2012. High capacity reversible data hiding scheme based upon discrete cosine transformation. J. Syst. Softw. 85 (10), 2395–2404.

Lin, Y., 2014. A data hiding scheme based upon DCT coefficient modification. Comput. Stand. Interfaces 36, 855–862.

Lu, T., Tseng, C., Wu, J., 2015. Dual imaging-based reversible hiding technique using LSB matching. Signal Process. 108, 77–89.

Malik, A., Sikka, G., Verma, K.H., 2015. A modified pixel-value differencing image steganographic scheme with least significant bit substitution method. I.J. Image Graph Signal Process. 4, 68–74.

Maniriho, P., Ahmad, T., 2017. A data hiding approach using enhanced-RDE in grayscale images. 2nd International Conference on Advanced Mechatronics, Intelligent Manufacture, and Industrial Automation (ICAMIMIA).

Mehdi, H., Mureed, H., 2013. A survey of image steganography techniques. Int. J. Adv. Sci. Technol. 54 (February), 1–12.

Nagaraj, V., Vijayalakshmi, V., Zayaraz, G., 2013. Color image steganography based on pixel value modification method using modulus function. IERI Proc. 4, 17–24.

Nguyen, T., Chang, C., Chang, W., 2016. Image Communication High capacity reversible data hiding scheme for encrypted images. Signal Process. Image Commun. 44, 84–91.

Parvez, M.T., Gutub, A.A., 2014. Vibrant color image steganography using channel differences and secret data distribution Vibrant Color Image Steganography using Channel. Kuwait J. Sci. Eng. (January 2014), 127–142

Peng, F., Li, X., Yang, B., 2012. Adaptive reversible data hiding scheme based on integer transform. Signal Process. 92 (1), 54–62.

Qian, Z., Zhang, X., 2012. Lossless data hiding in JPEG bitstream. J. Syst. Softw. 85 (2), 309–313.

Rahmani, V., Mohammad, M.P., 2017. High hiding capacity steganography method based on pixel indicator technique. In: 2017 5th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), pp. 144–149.

Rajput, M., Deshmukh, M., Nain, N., 2016. A novel approach for concealing image by utilizing the concept of secret sharing scheme and steganography. In: 2016 International Conference on Information Technology A, pp. 51–56.

Saleema, A., Amarunnishad, T., 2016. A new steganography algorithm using hybrid fuzzy neural networks. In: International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST-2015), pp. 1566–1574.

Shi, Y.-Q., Li, X., Zhang, X., Wu, H.-T., Bin, M., 2016. Reversible data hiding: advances in the past two decades. IEEE Access 4, 3210–3237.

Subhedar, M.S., Mankar, V.H., 2014. Current status and key issues in image steganography: a survey. Comput. Sci. Rev. 13–14 (2), 95–113.

Tang, M., Hu, J., Song, W., 2014. A high capacity image steganography using multi-layer embedding. Optik (Stuttg) 125 (15), 3972–3976.

Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst. Video Technol. 13 (8), 890–896.

Tsai, Y., Tsai, D., Liu, C., 2013. Reversible data hiding scheme based on neighboring pixel differences. Digit. Signal Process. 23 (3), 919–927.

Verma, V., Poonam, Chawla, R., 2014. An enhanced least significant bit steganography method using midpoint circle approach. In: International Conference on Communication and Signal Processing, pp. 105–108.

Wang, K., Lu, Z., Hu, Y., 2013. A high capacity lossless data hiding scheme for JPEG images. J. Syst. Softw. 86 (7), 1965–1975.

Xiao, D., Xiang, Y., Zheng, H., Wang, Y., 2017. Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism. J. Vis. Commun. Image Represent. 45, 1–10.

Yang, C.-H., 2008. Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recogn. 41 (8), 2674–2683.

Yaqub, M.K., Al-jaber, A., 2006. Reversible watermarking using modified difference expansion. Int. J. Comput. Inf. Sci. 4 (3), 134–142.

Yi, H., Wei, S., Jianjun, H., 2009. Improved reduced difference expansion based reversible data hiding scheme for digital images. In: 9th International Conference on Electronic Measurement & Instruments, pp. 315–318. ICEMI '09.

Yi, S., Zhou, Y., 2016. Binary-block embedding for reversible data hiding in encrypted images. Signal Process. 133 (September 2016), 40–51.

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

Zhang, X., Wang, S., 2006. "Efficient steganographic embedding by exploiting modification direction 10(11) (2006) 781–783.

Zhang, W., Ma, K., Yu, N., 2014. Reversibility improved data hiding in encrypted images $. Signal Process. 94, 118–127.