Sensing and Imaging (2021) 22:7
https://doi.org/10.1007/s11220-020-00328-w

ORIGINAL PAPER

Shadow Image Based Reversible Data Hiding Using Addition and Subtraction Logic on the LSB Planes

Monalisa Sahu[1] · Neelamadhab Padhy[1] · Sasanko Sekhar Gantayat[2] · Aditya Kumar Sahu[2]

Received: 11 February 2020 / Revised: 18 September 2020 / Accepted: 24 December 2020 /
Published online: 5 February 2021

Abstract

Image steganographic communication demands a fair trade-off among the three diametrically opposed metrics such as higher capacity, larger visual quality, and attack survival ability (ASA). Recently, some reversible data hiding (RDH) techniques using dual images have shown promising results to achieve the aforementioned needs. However, maintaining a balance among these metrics is still an open challenge. In this paper, using the concept of shadow image, which is basically the replica of the cover image (CI) and performing some simple addition and subtraction logic on the shadow image pixels, we propose an improved RDH technique that offers larger capacity, better stego-image (SI) quality and higher ASA. At first, during embedding, three shadow images of the CI are produced. Then, the shadow image pixels are adjusted based on their XOR features of the least significant bit planes. After embedding the secret bits, a maximum of ± 1 modification has been observed in the SI pixels. Later at the receiving end, the CI has been restored by applying the round function on the obtained SI pixels. Experimental results show that the proposed technique offers excellent visual quality with peak signal-to-noise ratio and structural similarity index (SSIM) of 52.47 dB, 53.91 dB, 52.48 dB and 0.9974, 0.9981, 0.9974 for the respective shadow images. Further, the proposed technique show exceptional anti-steganalysis ability to regular and singular analysis, pixel difference histogram analysis, and bit pair analysis. Additionally, the proposed technique successfully avoids the falling-off boundary problem.

Keywords Reversible data hiding · Image steganography · Capacity · Least significant bit

✉ Monalisa Sahu
monalisa.sahu@giet.edu

[1] School of Engineering and Technology (CSE), GIET University, Gunupur, Odisha 765022, India

[2] Department of Computer Science and Engineering, GMRIT, Rajam, Andhra Pradesh 532127, India

1 Introduction

Owing to the expeditious progress in the field of digitization, data hiding techniques have received a colossal interest from the researchers. In this regard, to achieve confidentiality to data during communication fields like watermarking, cryptography, and steganography have gained enormous responses from far and wide [1]. Watermarking is the process of embedding the secret information in a digital file, especially for ownership identification. On the other hand, the elemental goal of cryptography is to confound the burglar from understanding the communicated data. Contrarily, steganography doesn't give any indication of data communication to the invader. It obscures the secret data in a digital carrier [2]. Steganography, due to its feature of innocence, has drawn a massive response from the digital data hiding community. Here, the preferred media for communicating the essential information are the image. Besides the image, steganography can be also achieved using various digital objects like text, audio, and video [3].

In general, steganography is intended for those who wish to communicate in an entire cover-up manner. Basically, it can be furnished in spatial or transform domains. In the spatial domain, the IS techniques are majorly classified into either (1) reversible or (2) irreversible [4]. RDH techniques are primarily used in such applications where both the secret information as well as the original carrier image needs to be obtained. On the other hand, the underlying focus of the irreversible image steganography technique is to retrieve the concealed bits only. The potency of any image steganography technique is ascertained using various IS parameters like imperceptibility, capacity, and ASA. PSNR (Peak signal-to-noise ratio) is used to measure the imperceptibility [5]. Capacity refers to the maximum amount of secret bits an image can conceal. Finally, the ASA can be verified by applying various stego-attacks like RS analysis, PDH analysis, and bit pair analysis [6].

The reversible technique recovers the secret data as well as the CI at the recipient side successfully. Techniques like (1) difference expansion (DE), (2) histogram shifting (HS), and (3) dual image based techniques are presented by many authors in the literature. On the contrary, irreversible techniques focus on the successful retrieval of only the secret data. Various irreversible techniques such as (1) least significant bit (LSB) substitution, (2) pixel value differencing (PVD), (3) LSB + PVD, (4) PVD + modulus function (MF), and (5) exploiting modification direction (EMD) have been suggested by the researchers [7].

The conventional LSB based techniques offer good capacity when more number of LSB planes of the pixels are considered for embedding. However, LSB substitution techniques are exposed to RS analysis. Recently, an improved LSB substitution technique with a maximum of ± 1 modification in the SI has been proposed by Wu and Hwang [8]. Wang et al. [9] proposed a local pixel adjustment process (LPAP) using the moderately-significant-bit (MSB) technique to raise the visual quality of the SI. However, this technique incurs high computational complexity. Therefore, to reduce the complexity, Chang et al. [10] suggested a combination of LSB and encryption based technique. Once again, Wang

et al. [11] introduced the perceptual modeling strategy based modified LSB technique to improve the visual quality of SI compared to conventional LSB based techniques. A novel data mapping strategy to improve the capacity utilizing the MSB and LSB of the CI pixels has been proposed by Zakaria et al. [12]. Unlike conventional LSB substitution technique, this technique showed excellent ASA to RS as well as histogram attack. The noise non-sensitive regions of the image can resist more embedding as compared to the noise-sensitive regions. With this idea, an adaptive LSB based technique to increase the capacity with accepted SI quality has been reported by Yang et al. [13]. The LSB Substitution based techniques directly substitute the LSBs with the embedding bits. Therefore, these techniques are exposed to various statistical steganalysis like RS and bit plane analysis. Sharp [14] introduced an embedding technique which at best modifies the CI pixels to ± 1 only for embedding the secret bits. This technique later called LSB matching [15]. Wu and Tsai [16] introduced the concept of PVD, where the texture regions of the image can resist potentially more embedding bits than the smoother regions. This technique utilizes the fluctuation or difference between the two successive pixels (SPs) for embedding the secret bits. Wu and Tsai's [16] technique successfully resists the RS attack. However, this technique suffers from two issues, such as (1) FOBP and (2) the presence of secret bits are exposed to PDH attack. FOBP issue arises when the SI pixel exceeds the allowable range {0 to 255} for the pixels. Thus the FOBP pixels cannot be utilized for embedding the secret bits. Recently, some improved PVD based techniques [17–21] were suggested by the researchers. The idea of combining LSB and PVD techniques to promote the capacity was initially formed by Wu et al. [22]. In this technique, the SPs are partitioned into different blocks. Then, the fluctuation among the SPs for each block is calculated. Then, using this fluctuation value (FV), the smoother or edge blocks are identified. LSB substitution is applied to the smoother and PVD is applied to the edge blocks. Yang et al. [23] found Wu et al.'s [22] LSB + PVD technique is more conformable to LSB substitution technique and therefore, the technique is exposed to RS analysis. Further, they have suggested a modified range criteria to choose the smooth and edge blocks. Khodaei and Faez [24] partitioned the CI into different blocks with three SPs each. Then 3LSB substitution is applied to the reference pixel which is the central pixel and the PVD technique is applied to other two pixels. This technique reportedly improves the capacity compared to Wu et al.'s [22] technique. Further, the ASA against RS analysis is superior for this technique. Some more LSB + PVD based techniques are presented in [23–29]. Wang et al. [30] avoided the FOBP issue by bringing together both PVD and MF strategy. Also, this technique offers larger capacity compared to Wu and Tsai's [16] technique. Further, this technique shows good ASA to RS analysis. Joo et al. [31] pointed out the weakness of Wang et al.'s [30] technique to PDH analysis. They found abnormal fluctuation in the PVD histogram of the SI with Wang et al.'s [30] technique. Further, they addressed this issue by proposing a novel PVD + MF based technique using turnover policy and pixel readjustment process. Other improved PVD + MF based techniques are suggested in [32–36].

In many real-time applications such as electronic health care infrastructure, medical image processing, military communications, and IoT supported devices,

retrieving both the embedded data as well as the carrier object is essential. The idea of RDH was first coined by Barton [37]. Later, Tian's [38] difference expansion (DE) based technique was among the first initial steps towards RDH applications. The DE based technique performs with the idea of expanding the FV between the two SPs for creating larger embedding space. Alattar [39] improved the capacity compared to Tian's [38] technique using four pixels based two-fold expansion strategy. Kim et al. [40] suggested an improved DE technique utilizing the location map to increase the capacity compared to Tian's [38] technique. Besides DE, another efficient RDH technique is HS. It was first devised by Ni et al. [41]. HS based techniques find the highest point of the histogram to embed the secret bits. Later, to further raise the capacity compared to Ni et al. [41] technique, Tsai et al. [42] utilized pixel overlapping technique. Recently, dual image based reversible techniques has drawn great interest among the researchers. In this regard, Lu et al. [43] have extended Mielikainen's [15] LSB matching technique to raise the capacity as well as to achieve the reversibility. Authors in [44–47] have suggested various reversible techniques using two or more images.

2 Research Contribution

The proposed reversible technique is based on the concept of the shadow image. A shadow image is a mirror image of the CI. There are three shadow images are produced from each CI. Then, embedding is performed on the LSB planes of the pixels using the XOR feature. The significant contributions of the proposed technique are as follows:

(1) The proposed shadow image based reversible technique maintains a fair trade-off between the conflicting metrics such as imperceptibility, capacity, and ASA.
(2) Further, the proposed technique shows excellent anti-steganalysis ability to various steganalysis attacks.
(3) Finally, the proposed technique successfully avoids the FOBP.

The remainder of this paper is organized as follows. Section 3 reviews the conventional 2LSB substitution technique, Mielikainen's [15] LSB matching technique, Wu and Tsai's [16] PVD technique, and Wu and Hwang's [8] technique. The proposed embedding and extraction procedures are depicted at length in Sect. 4. Section 5 presents the experimental results of the proposed and some other related works. Finally, conclusions are drawn in Sect. 6.

3 Related Work

In this section, some classical data hiding techniques are briefly reviewed. Also, the underlying issues of each of them are highlighted. At first, the 2LSB substitution technique is discussed with an illustration. Then the embedding and

extraction steps of the PVD technique proposed by Wu and Tsai [16] are discussed. Further, an illustration of the PVD technique, as well as the FOBP issue is also presented. Next, Mielikainen's [15] LSB matching technique is also briefly explained. Finally, Wu and Hwang's [8] technique is outlined with its issues.

3.1 LSB substitution Technique

LSBS technique is by far the simplest technique that was introduced by [48]. In this technique, the LSBs are simply substituted with the secret bits to be embedded. The capacity increases when more number of LSBs are substituted with the embedding bits. An illustration demonstrating the 2LSB substitution technique has been shown in Fig. 1. It is self-explanatory.

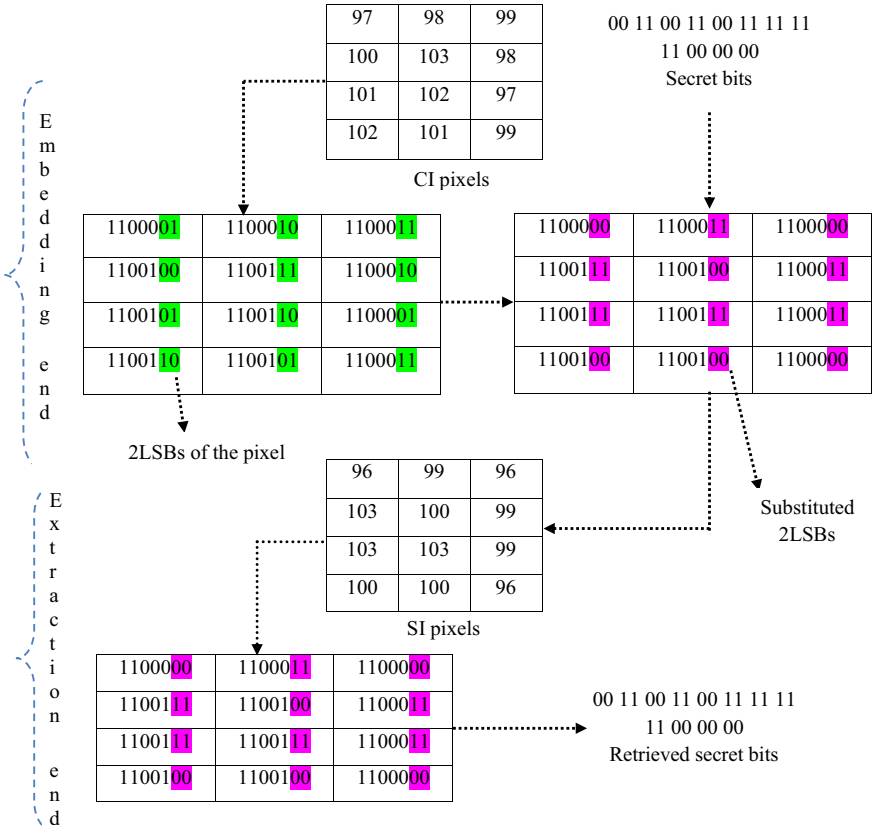


Fig. 1 An illustration of the embedding and extraction process for the 2LSB substitution technique

3.1.1 Issues of LSB Substitution Technique

1. The conventional LSB substitution techniques suffer from low visual SI quality.
2. Further, these techniques are exposed to most of the statistical steganalysis like RS, chi-square, and bit plane analysis.

3.2 Mielikainen's [15] LSB Matching Technique

The LSB matching approach proposed by Mielikainen [15] randomly modify the pixel value by ± 1. In this approach, each pixel hides 1 bit of secret data. At first, two pixels and two secret bits are taken. Then, the LSB bits for the pixels are compared with the secret bits and are readjusted. The pixels are readjusted using the function F(.). Assume c_1 and c_2 be the two cover image pixels and b_1 and b_2 be the two secret bits. The function $F(c_1, c_2)$ can be defined using Eq. (1).

$$F(c_1, c_2) = \text{LSB}\left(\lfloor c_1/2 \rfloor + c_2\right) \tag{1}$$

The secret bits are embedded using the following steps.

Step 1 When $\text{LSB}(c_1) = b_1$ and $F(c_1, c_2) = b_2$, then no modifications required, i.e., the stego-pixels $c_1^* = c_1$ and $c_2^* = c_2$.

Step 2 When $\text{LSB}(c_1) = b_1$ and $F(c_1, c_2) \neq b_2$, then set the pixel $c_1^* = c_1$ and $c_2^* = c_2 + 1$.

Step 3 When $\text{LSB}(c_1) \neq b_1$ and $F(c_1 - 1, c_2) = b_2$, then set the pixel $c_1^* = c_1 - 1$ and $c_2^* = c_2$.

Step 4 When $\text{LSB}(c_1) \neq b_1$ and $F(c_1 - 1, c_2) \neq b_2$, then set the pixel $c_1^* = c_1 + 1$ and $c_2^* = c_2$.

At the time of extraction, the secret bit b_1 can be obtained by finding the LSB of c_1^*. Similarly, b_2 can be retrieved using $b_2 = \text{LSB}(\lfloor c_1^*/2 \rfloor + c_2^*)$.

3.2.1 Issue of Mielikainen's [15] LSB Matching Technique

1. This technique embeds only 1 bit in each pixel of the CI. Therefore, low capacity remains the biggest challenge for this technique.

3.3 Wu and Tsai's [16] PVD Technique

An image consists of edge and smooth regions. The edge regions of the image can resist potentially more number of secret bits than that of the smoother one. Wu and Tsai [16] proposed the concept of PVD steganography which utilizes the idea of pixel difference. At first, the image is divided into blocks with two successive pixels (SPs) each. Then, the fluctuation values (FVs) between the SPs for each block are obtained. Later using these FVs, data embedding is performed. The embedding and extraction steps for Wu and Tsai's [16] technique are discussed below followed by an illustration in Fig. 2.

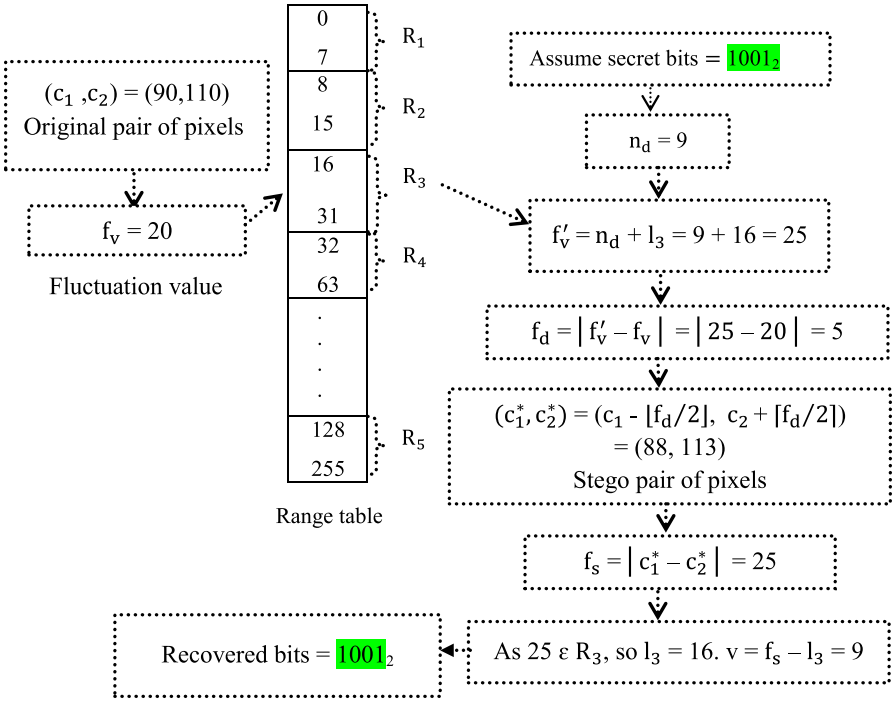


Fig. 2 An illustration of embedding and extraction process for the PVD technique [16]

3.3.1 PVD Embedding Steps

Step 1 Let (c_1, c_2) be the two SPs of the first block of a CI.

Step 2 The FVs for each block can be obtained using $f_v = |c_1 - c_2|$. Then, using f_v the number of embedding bits (n) is obtained using Eq. (2).

$$n = \log_2 \left(u_i - l_i + 1 \right) \tag{2}$$

where l_i and u_i are the respective lower and upper bounds for the range R_i in Table 1.

Table 1 Range table for Wu and Tsai's [16] PVD technique

Range(R_i) = (l_i ,u_i)	$R_1 \in [0,7]$	$R_2 \in [8,15]$	$R_3 \in [16,31]$	$R_4 \in [32,63]$	$R_5 \in [64, 127]$	$R_6 \in [128, 255]$
Width	8	8	16	32	64	128
Embedding length (n)	3	3	4	5	6	7

Step 3 Now obtain the decimal for the n bits. Let it be n_d. Then, obtain $f_v^{'}$ using Eq. (3)

$$f_v^{'} = n_d + l_i \tag{3}$$

Step 4 Find f_d as the difference between f_v and $f_v^{'}$ as $f_d = \left|f_v^{'} - f_v\right|$.

Step 5 Apply Eq. (4) to find the SI pixels as (c_1^*, c_2^*).

$$(c_1^*, c_2^*) = \begin{cases} \left(c_1 + \lceil f_d/2 \rceil,\ c_2 - \lfloor f_d/2 \rfloor\right), \text{ if } c_1 \geq c_2 \text{ and } f_v^{'} > f_v \\ \left(c_1 - \lfloor f_d/2 \rfloor,\ c_2 + \lceil f_d/2 \rceil\right), \text{ if } c_1 \langle c_2 \text{ and } f_v^{'} \rangle f_v \\ \left(c_1 - \lceil f_d/2 \rceil,\ c_2 + \lfloor f_d/2 \rfloor\right), \text{ if } c_1 \geq c_2 \text{ and } f_v^{'} \leq f_v \\ \left(c_1 + \lceil f_d/2 \rceil,\ c_2 - \lfloor f_d/2 \rfloor\right), \text{ if } c_1 < c_2 \text{ and } f_v^{'} \leq f_v \end{cases} \tag{4}$$

Here $\lceil f_d/2 \rceil$ is the ceiling value of $f_d/2$ and $\lfloor f_d/2 \rfloor$ is the floor value of $f_d/2$.

Step 6 Embedding is completed.

3.3.2 PVDS Extraction Steps

Step 1 At the receiving end, at first obtain the stego-pixels (c_1^*, c_2^*) from the first block of the SI.

Step 2 Then, find the fluctuation between these two stego-pixels as $f_s = \left|c_1^* - c_2^*\right|$. Now using this f_s, obtain its l_i and u_i from the range table. Again, obtain the difference between f_s and it's corresponding lower bound l_i as in Eq. (5).

$$v = \left|f_s - l_i\right| \tag{5}$$

Finally, represent v in n binary bits where $n = \log_2\left(u_i - l_i + 1\right)$. These are the extracted secret bits.

Step 3 Extraction is completed.

3.3.3 Issues of Wu and Tsai's [16] PVD Technique

1. Wu and Tsai's [16] PVD technique suffer from the FOBP issue. In fact, most of the PVD based techniques usually suffer from this issue. Therefore, the capacity remains an issue for these techniques. Figure 3 shows an illustration of FOBP in this technique.
2. Next, this technique observes abnormal behavior to the histogram analysis leading to expose the presence of secret information.

3.4 Wu and Hwang's [8] Improved LSB (ILSB) Technique

Wu and Hwang [8] suggested an improved LSB technique that produces imperceptible SI compared to other state-of-art LSB based techniques. Here, embedding is performed in the block consisting of three pixels each. In this technique, a block of three pixels embeds three bits of secret data. Therefore Wu and Hwang's [8] technique endure from low capacity. Following this, a brief discussion with a pictorial illustration in Fig. 4 is presented below. Consider c_1, c_2 and c_3 be the three SPs of a block. Let $c_1{=}c_1^1c_1^2c_1^3c_1^4c_1^5c_1^6c_1^7c_1^8$, $c_2{=}c_2^1c_2^2c_2^3c_2^4c_2^5c_2^6c_2^7c_2^8$ and $c_3{=}c_3^1c_3^2c_3^3c_3^4c_3^5c_3^6c_3^7c_3^8$ be the binary representation of these pixels. Now, find the values of P, Q, R using Eq. (6).

$$(P, Q, R) = \left(c_1^8 \oplus c_1^7 \oplus c_2^8, c_2^8 \oplus c_2^7 \oplus c_3^8, c_3^8 \oplus c_3^7 \oplus c_1^8\right) \tag{6}$$

Assume b_1, b_2 and b_3 be the embedding bits. Now, modify c_1, c_2 and c_3 by performing the pixel adjustment steps to obtain the stego-pixels as s_1, s_2, and s_3. During extraction, to obtain the secret bits b_1, b_2 and b_3 from the SI pixels using the same Eq. (6).

3.4.1 Issues of Wu and Hwang's [8] Technique

1. Wu and Hwang's [8] technique offers excellent SI quality at the cost of capacity, i.e., this technique embeds only 1 bit in each pixel. Therefore the capacity of Wu and Hwang's [8] technique is very low.

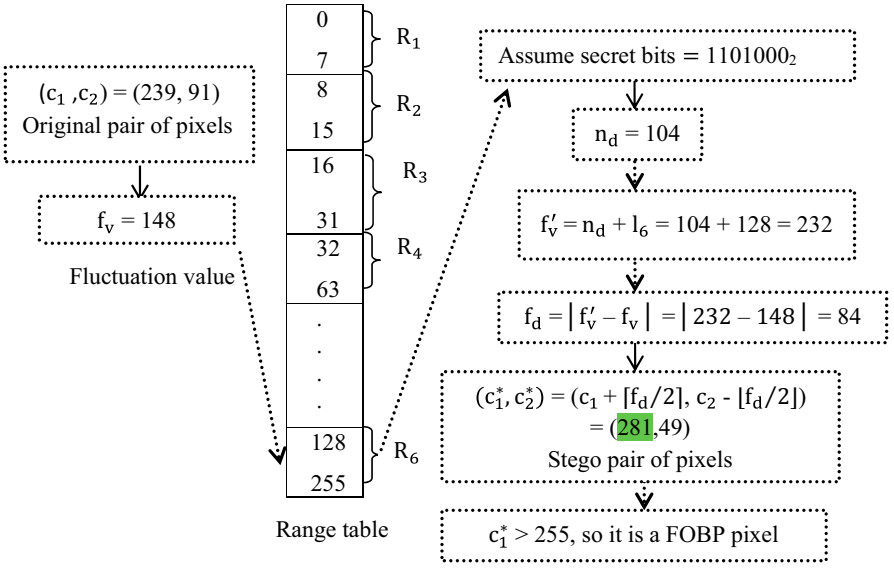


Fig. 3 An illustration of FOBP pixel in Wu and Tsai's [16] PVD technique

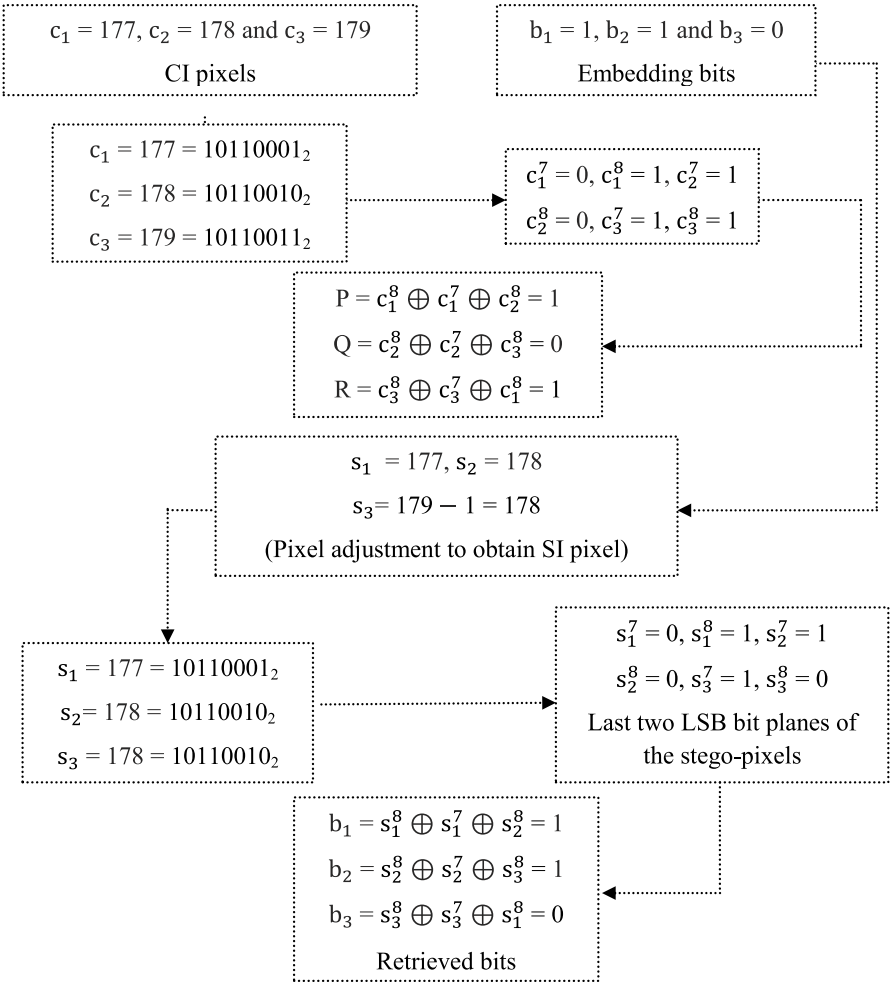


Fig. 4 An illustration of the embedding and extraction for Wu and Hwang's [8] technique

2. Further, Wu and Hwang's [8] technique is irreversible. Therefore, this technique is not suitable in such applications that require the carrier object also needs to be completely restored.

4 Proposed Technique

In this section, we propose the embedding and extraction procedure of our proposed technique. Before embedding, three identical images of the CI known as the shadow images are obtained. The shadow images consist of the exact pixels or replica of the CI. The secret bits are embedded in the shadow images to produce the SI. The following are some silent features of the proposed technique.

1. The proposed technique successfully restores the CI at the recipient end. Therefore, complete reversibility is achieved.
2. Again, the proposed technique conceals the secret bits with maximum modification of ± 1 to the shadow image pixels. Therefore, the visual quality of the SI is optimal.
3. Also, all the three shadow images are utilized for embedding the secret bits. Therefore, someone without one of the SI cannot accurately retrieve the secret information.

Now, we narrate the embedding and extraction procedures of the proposed techniques. Figure 5 shows the pictorial representation of embedding, extraction, and CI image pixel restoration procedure for the proposed technique. Further, Fig. 6 shows an illustration of the technique. The explanation of Fig. 6 is done in Sect. 3.1.

4.1 Embedding Procedure

The CI consisting of the pixels $\sum_{n=1}^{H\times W} C_n$, where 'H' and 'W' denotes the height and width of the image. Here the embedding procedure is explained for one of the CI pixels C_1. Let the three shadow images be U_1, V_1 and W_1. Assume the pixels of U_1 are $\sum_{n=1}^{H\times W} u_n^1$, V_1 are $\sum_{n=1}^{H\times W} v_n^1$ and W_1 are $\sum_{n=1}^{H\times W} w_n^1$. Assume the embedding bits are $\sum_{n=1}^{k} b_n$. u_1^1, v_1^1 and w_1^1 be the respective first pixels of the shadow images U_1, V_1 and W_1. These three shadow image pixels embeds three secret bits. Let the three secret bits be b_1, b_2 and b_2.

Step 1 At first, convert u_1^1, v_1^1 and w_1^1 to their respective eight-bit binary as given below.

$u_1^1 = u(1,8),\ u(1,7),\ u(1,6),\ u(1,5),\ u(1,4),\ u(1,3),\ u(1,2),\ u(1,1).$
$v_1^1 = v(1,8),\ v(1,7),\ v(1,7),\ v(1,6),\ v(1,5),\ v(1,4),\ v(1,3),\ v(1,2),\ v(1,1).$
$w_1^1 = w(1,8),\ w(1,7),\ w(1,6),\ w(1,5),\ w(1,4),\ w(1,3),\ w(1,2), w(1,1).$

Step 2 Here, $u(1,8)$, $v(1,8)$, $w(1,8)$ and $u(1,1)$, $v(1,1)$, $w(1,1)$ denotes the respective most and least significant bits of the shadow image pixels u_1^1, v_1^1 and w_1^1.

Step 3 Then using the XOR operation on the last two LSBs of the respective shadow image pixels obtain the variables V_{12}, V_{23} and V_{31} using Eqs. (7), (8) and (9). Here V_{12} is obtained by performing the XOR of the last two LSBs of u_1^1 and LSB of v_1^1. V_{23} is obtained by performing the XOR of the last two LSBs of v_1^1 and LSB of w_1^1. Similarly, V_{31} is obtained by performing the XOR of the last two LSBs of w_1^1 and LSB of u_1^1.

$$V_{12} = u(1,2) \oplus u(1,1) \oplus v(1,1) \tag{7}$$

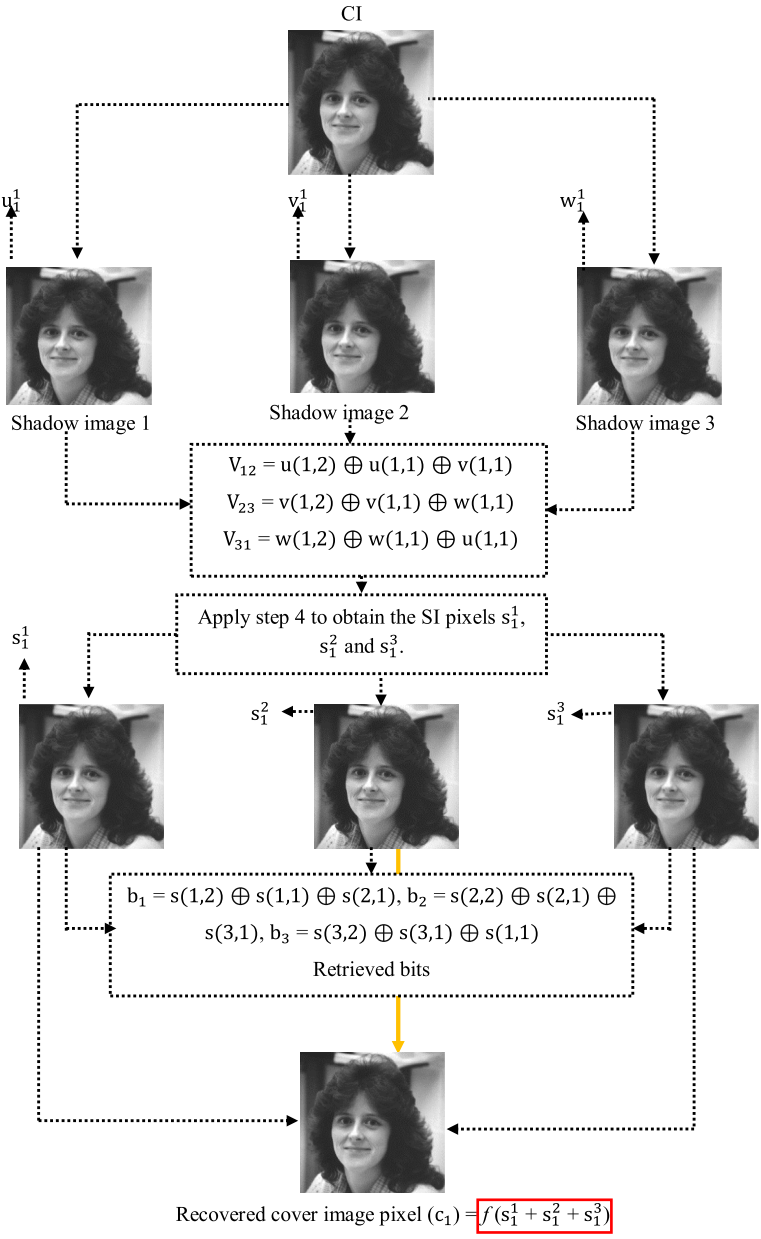


Fig. 5 Pictorial representation of embedding, extraction and original image pixel restoration procedure for the proposed technique

$$V_{23} = v(1,2) \oplus v(1,1) \oplus w(1,1) \tag{8}$$

$$V_{31} = w(1,2) \oplus w(1,1) \oplus u(1,1) \tag{9}$$

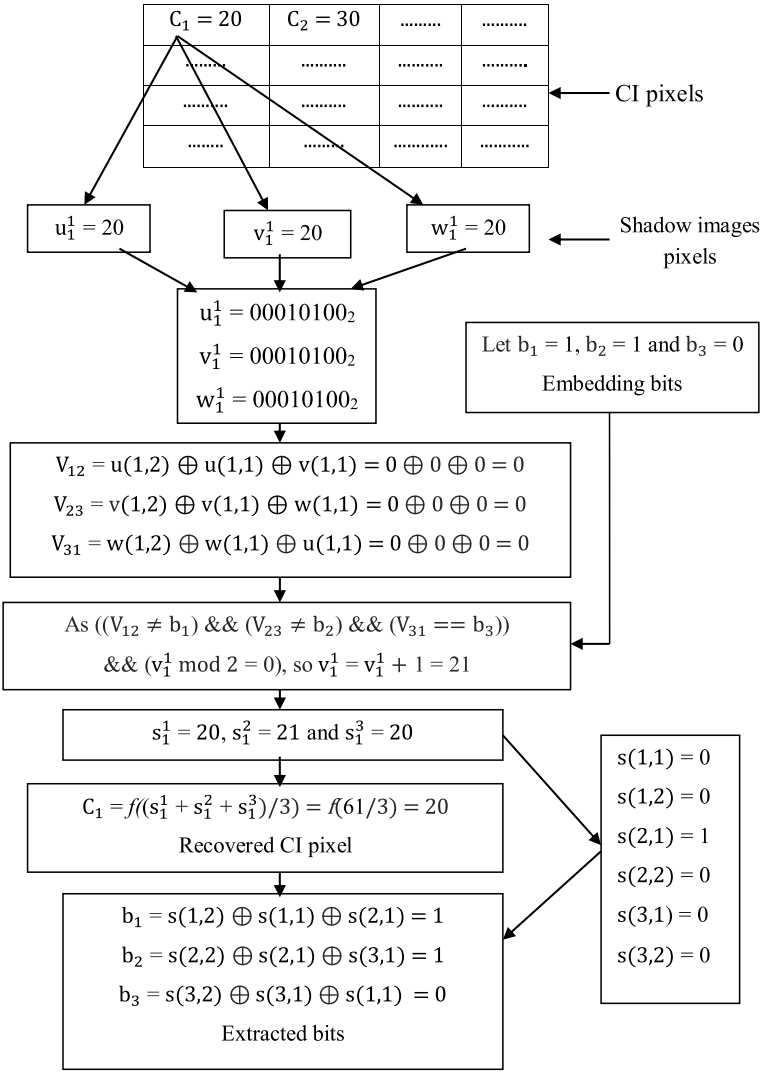


Fig. 6 An illustration of the embedding, extraction, and restoration for the proposed technique

Step 4 Now readjust the pixels by performing following If Else loop.

If $(V_{12} == b_1)$ && $(V_{23} == b_2)$ && $(V_{31} == b_3)$.
Then $u_1^1 = u_1^1$, $v_1^1 = v_1^1$ and $w_1^1 = w_1^1$.

Else If $((V_{12} \neq b_1)$ && $(V_{23} == b_2)$ && $(V_{31} == b_3))$ && (If $v_1^1 \bmod 2 = 0$).
Then $v_1^1 = v_1^1 - 1$.
Else $v_1^1 = v_1^1 + 1$.

End

Else If (($V_{12} == b_1$) && ($V_{23} \neq b_2$) && ($V_{31} == b_3$)) && (If w_1^1 mod 2 = 0).
Then $w_1^1 = w_1^1 - 1$
Else $w_1^1 = w_1^1 + 1$.

End

Else If (($V_{12} == b_1$) && ($V_{23} == b_2$) && ($V_{31} \neq b_3$)) && (If u_1^1 mod 2 = 0).
Then $u_1^1 = u_1^1 - 1$.
Else $u_1^1 = u_1^1 + 1$.

End

Else If (($V_{12} \neq b_1$) && ($V_{23} \neq b_2$) && ($V_{31} == b_3$)) && (If v_1^1 mod 2 = 0).
Then $v_1^1 = v_1^1 + 1$.
Else $v_1^1 = v_1^1 - 1$.

End

Else If (($V_{12} == b_1$) && ($V_{23} \neq b_2$) && ($V_{31} \neq b_3$)) && (If w_1^1 mod 2 = 0).
Then $w_1^1 = w_1^1 + 1$.
Else $w_1^1 = w_1^1 - 1$.

End

Else If (($V_{12} \neq b_1$&& ($V_{23} == b_2$) && ($V_{31} \neq b_3$)) && (If u_1^1 mod 2 = 0).
Then $u_1^1 = u_1^1 + 1$.
Else $u_1^1 = u_1^1 - 1$.

End

Else If (($V_{12} \neq b_1$) && ($V_{23} \neq b_2$) && ($V_{31} \neq b_3$)) && (If w_1^1 mod 2 = 0).
Then $w_1^1 = w_1^1 - 1$.
Else $w_1^1 = w_1^1 + 1$.

End

If u_1^1 mod 2 = 0.
Then $u_1^1 = u_1^1 + 1$.
Else $u_1^1 = u_1^1 - 1$.

End

演算法有小錯誤，需要移到上面。

Step 5 Finally, obtain the SI pixels for the respective shadow image pixels as $s_1^1 = u_1^1$, $s_1^2 = v_1^1$ and $s_1^3 = w_1^1$.

Step 6 Embedding is completed.

4.2 Extraction Procedure

Step 1 At the receiver side, obtain the SI pixels as s_1^1, s_1^2 and s_1^3.

Step 2 Then convert s_1^1, s_1^2 and s_1^3 to their respective eight-bit binary as given below.

$s_1^1 = s(1,8),\ s(1,7),\ s(1,6),\ s(1,5),\ s(1,4),\ s(1,3),\ s(1,2),\ s(1,1).$
$s_1^2 = s(2,8),\ s(2,7),\ s(2,6),\ s(2,5),\ s(2,4),\ s(2,3),\ s(2,2),\ s(2,1).$
$s_1^3 = s(3,8),\ s(3,7),\ s(3,6),\ s(3,5),\ s(3,4),\ s(3,3),\ s(3,2),\ s(3,1).$

Step 3 Now to retrieve the secret bits b_1, b_2 and b_3 from the stego-pixels using the Eqs. (10), (11) and (12).

$$b_1 = s(1,2) \oplus s(1,1) \oplus s(2,1) \tag{10}$$

$$b_2 = s(2,2) \oplus s(2,1) \oplus s(3,1) \tag{11}$$

$$b_3 = s(3,2) \oplus s(3,1) \oplus s(1,1) \tag{12}$$

Finally, obtain the OI pixel C_1 using Eq. (13)

$$C_1 = f\left(s_1^1 + s_1^2 + s_1^3\right) \tag{13}$$

where the function '*f*' is the round function.

Step 4 Extraction is completed.

4.3 An Illustration of the Proposed Technique

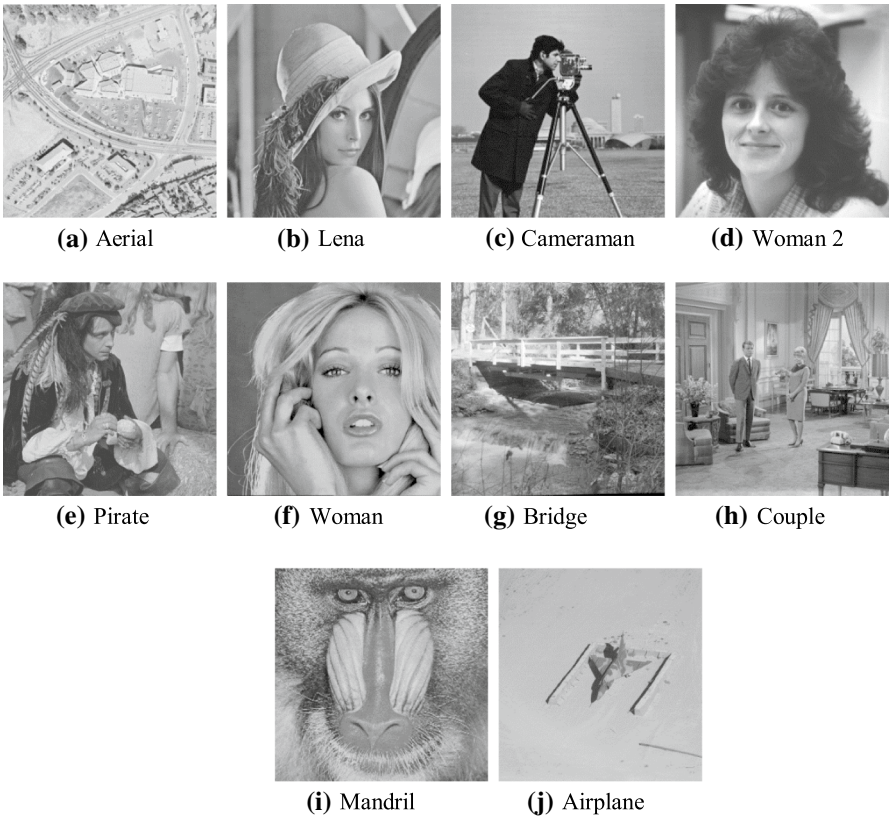
Considering Fig. 6, an explanation of the illustration for the proposed technique is presented in this section. Let C_1 be one of the CI pixel. Assume $C_1 = 20$ and the three shadow image pixels of C_1 be u_1^1, v_1^1 and w_1^1. Since the shadow image pixels are the copy of the CI pixel, therefore, the values of $u_1^1 = 20$, $v_1^1 = 20$ and $w_1^1 = 20$. The eight-bit binary of u_1^1, v_1^1 and w_1^1 are 00010100_2, 00010100_2 and 00010100_2 respectively. Assume the embedding bits be $b_1 = 1$, $b_2 = 1$ and $b_3 = 0$. Now using Eqs. (7), (8) and (9) the values for V_{12}, V_{23} and V_{31} are obtained as 0, 0 and 0 respectively. In Step 4 of the embedding procedure, the condition $((V_{12} \neq b_1)$ && $(V_{23} \neq b_2)$ && $(V_{31} == b_3))$ && (If $v_1^1 \bmod 2 = 0$) is satisfied. Hence, $v_1^1 = v_1^1 + 1 = 21$. Finally, the stego-pixels for the CI pixel $C_1 = 20$ are $s_1^1 = u_1^1 = 20$, $s_1^2 = v_1^1 = 21$ and $s_1^3 = w_1^1 = 20$. At the receiving end, the stego-pixels are converted to its eight-bit binary as 00010100_2, 00010101_2 and 00010100_2. Then, using Eqs. (10), (11) and (12) the embedding bits are extracted as 1, 1 and 0. Finally, the CI pixel is restored using the Eq. (13) (Fig. 7).

5 Experimental Results and Discussion

The experiment has been performed using MATLAB 2015(a). The grayscale images with the size of 512×512 have been taken from the USC-SIPI image database [49]. The obtained results for the capacity, imperceptibility parameters such as mean square error (MSE), PSNR, and structural similarity index (SSIM) are compared with various state-of-art techniques. Further, the FOBP for the proposed and other techniques are also calculated. The ASA has been tested by applying RS analysis, PDH analysis, and bit pair analysis. PSNR measures the SI quality in decibel (dB) [50]. The SI quality is better when the PSNR is high [51–53]. This can be computed using Eq. (14).

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\mathrm{MSE}} \tag{14}$$

where the mean square error (MSE) can be found using Eq. (15).



(a) Aerial **(b)** Lena **(c)** Cameraman **(d)** Woman 2

(e) Pirate **(f)** Woman **(g)** Bridge **(h)** Couple

(i) Mandril **(j)** Airplane

Fig. 7 The CIs (**a**–**j**) utilized for computing the results for the proposed and other techniques

$$\mathrm{MSE} = \frac{1}{x \times y} \Sigma_{i=1}^{x} \Sigma_{j=1}^{y} \left(C_{ij} - S_{ij}\right)^2 \tag{15}$$

where C_{ij} and S_{ij} are the pixels of CI and SI at (ith and jth) position respectively.

SSIM finds the similarity between the CI and the SI. It can be calculated using Eq. (16). SSIM value ranges from − 1 to 1, where 1 refers to optimal and − 1 refers to the worst similarity between CI and SI [54–56].

$$\mathrm{SSIM} = \frac{\left(2P_c Q_s + k_1\right)\left(2\sigma_{cs} + k_2\right)}{\left(P_c^2 Q_s^2 + k_1\right)\left(\sigma_c^2 + \sigma_s^2 + k_2\right)} \tag{16}$$

For the CI, P_C, P_C^2 and σ_C^2 are the mean, variance, and standard deviation. At the same time, for the SI, the Q_s, Q_s^2 and σ_s^2 are mean, variance, and standard deviation. σ_{cs} is the covariance between the CI and the SI. The constant $k_1 = c_1 L$ and $k_2 = c_2 L$, where $c_1 = 0.01$, $c_2 = 0.03$ and L is 255.

Tables 2, 3, 4, 5, 6, 7 and 8 presents the results of MSE, PSNR, capacity, and the number of FOBP pixels for the proposed and other state-of-art techniques such as 1LSB, 2LSB, 3LSB, Wu and Hawang's [8] technique, Wu and Tsai's [16] technique, Khodai and Faez's [24] technique, Mielikainen's [15] LSB matching technique, and Lu et al.'s [43] technique. The proposed technique produces three different SIs, and therefore, three different MSE and PSNR values are obtained and that are represented as MSE(1), MSE(2), MSE(3) and PSNR(1), PSNR(2), PSNR(3). Among all the techniques, Khodai and Faez's [24] technique hides the largest number of secret bits with 794,427 bits. However, this technique suffers from both FOBP as well as weakness to PDH analysis. Next, the 3LSB substitution technique offers a comparative larger capacity with 786,432 bits. However, the PSNR for the 3LSB technique remains low with 37.87 dB. When we compare the PSNR, Mielikainen's [43] technique, Wu and Hawang's [8] technique and 1LSB technique offer more than 50 dB. However, low capacity for these techniques remains the biggest challenge. Further, the 2LSB substitution technique and Lu et al. [43] technique both offer an acceptable capacity of 524,288 bits. At the same time, the LSB substitution techniques are exposed to RS attack. The PSNR for Wu and Tsai's [16] technique is acceptable but it has the drawback of low capacity, FOBP and weakness to PDH analysis. On the other hand, the proposed technique offers exceptional results for all the metrics. The PSNR for all the obtained SIs exceeds above 52 dB. Therefore, excellent visual qualities in the SIs are achieved. Similarly, the capacity is also good with 786,432 bits. Additionally, the proposed technique does not exceed the upper and lower boundary values for the pixels after embedding. Therefore, FOBP is successfully ruled out. From the above discussion, it can be concluded that the proposed technique is superior to its counterparts in terms of providing a good balance between capacity and imperceptibility.

Figures 8 and 9 present the pictorial comparison of the results for the propose and other techniques for the capacity and PSNR.

Table 2 Results of MSE, PSNR, and capacity for the proposed technique

Image size (512×512)	MSE(1)	MSE(2)	MSE(3)	PSNR(1)	PSNR(2)	PSNR(3)	Capacity
Aerial	0.37	0.27	0.37	52.48	53.89	52.48	786,432
Lena	0.37	0.27	0.37	52.48	53.89	52.48	786,432
Cameraman	0.37	0.27	0.37	52.49	53.89	52.48	786,432
Woman2	0.37	0.26	0.37	52.45	53.92	52.49	786,432
Pirate	0.37	0.26	0.37	52.48	53.92	52.49	786,432
Woman	0.37	0.26	0.37	52.50	53.92	52.50	786,432
Bridge	0.37	0.26	0.37	52.46	53.92	52.46	786,432
Couple	0.37	0.26	0.37	52.46	53.92	52.48	786,432
Mandril	0.37	0.26	0.37	52.47	53.91	52.47	786,432
Airplane	0.37	0.26	0.37	52.46	53.90	52.47	786,432
Average	0.37	0.26	0.37	52.47	53.91	52.48	786,432

MSE(1), MSE(2) and MSE(3) refers to the MSE values for the first, second and third SI respectively, PSNR(1), PSNR(2) and PSNR(3) refers to the PSNR values for the first, second and third SI respectively

Table 3 Results of SSIM and number of FOBP pixels for the proposed technique

Image size (512×512)	SSIM(1)	SSIM(2)	SSIM(3)	FOBP(1)	FOBP(2)	FOBP(3)
Aerial	0.9984	0.9989	0.9984	0	0	0
Lena	0.9970	0.9978	0.9970	0	0	0
Cameraman	0.9962	0.9973	0.9962	0	0	0
Woman2	0.9960	0.9972	0.9961	0	0	0
Pirate	0.9977	0.9983	0.9977	0	0	0
Woman	0.9975	0.9982	0.9975	0	0	0
Bridge	0.9990	0.9992	0.9990	0	0	0
Couple	0.9981	0.9986	0.9981	0	0	0
Mandril	0.9987	0.9991	0.9987	0	0	0
Airplane	0.9954	0.9967	0.9954	0	0	0
Average	0.9974	0.9981	0.9974	0	0	0

SSIM(1), SSIM(2) and SSIM(3) refers to the SSIM values for the first, second and third SI respectively, FOBP(1), FOBP(2) and FOBP(3) refers to the FOBP values for the first, second and third SI respectively

5.1 Security Analysis Against Various Attacks

In this section, the ASA of the proposed and other techniques to RS, PDH, and bit plane analysis are presented.

5.1.1 ASA Against RS Analysis

This section discusses the ASA of the proposed as well as the LSB substitution techniques to RS analysis. RS analysis is a well-known statistical test developed by Fridrich [57]. In this test, the pixels are grouped into two different groups such as, (1) the

Table 4 Results of 1LSB and 2LSB technique

Image size (512×512)	MSE	PSNR	SSIM	Capacity	FOBP	MSE	PSNR	SSIM	Capacity	FOBP
Aerial	0.50	51.13	0.9978	262,144	0	2.56	44.06	0.9893	524,288	0
Lena	0.50	51.14	0.9959	262,144	0	2.55	44.07	0.9796	524,288	0
Cameraman	0.50	51.14	0.9949	262,144	0	2.55	44.07	0.9750	524,288	0
Woman2	0.50	51.16	0.9947	262,144	0	2.55	44.07	0.9737	524,288	0
Pirate	0.50	51.15	0.9969	262,144	0	2.53	44.10	0.9847	524,288	0
Woman	0.50	51.12	0.9966	262,144	0	2.56	44.04	0.9828	524,288	0
Bridge	0.50	51.18	0.9990	262,144	0	1.85	45.45	0.9953	524,288	0
Couple	0.50	51.14	0.9974	262,144	0	2.55	44.06	0.9871	524,288	0
Mandril	0.50	51.15	0.9983	262,144	0	2.55	44.06	0.9913	524,288	0
Airplane	0.50	51.16	0.9941	262,144	0	2.76	43.72	0.9697	524,288	0
Average	0.50	51.15	0.9966	262,144	0	2.50	44.17	0.9829	524,288	0

Table 5 Results of 3LSB and Wu and Hawang's [8] technique

Image size (512×512)	MSE	PSNR	SSIM	Capacity	FOBP	MSE	PSNR	SSIM	Capacity	FOBP
Aerial	10.59	37.88	0.9597	786,432	0	0.33	52.91	0.9986	262,144	0
Lena	10.61	37.88	0.9225	786,432	0	0.33	52.91	0.9973	262,144	0
Cameraman	10.66	37.85	0.9119	786,432	0	0.33	52.91	0.9966	262,144	0
Woman2	10.52	37.90	0.9054	786,432	0	0.33	52.90	0.9964	262,144	0
Pirate	10.81	37.79	0.9401	786,432	0	0.33	52.90	0.9979	262,144	0
Woman	10.75	37.82	0.9337	786,432	0	0.33	52.92	0.9977	262,144	0
Bridge	9.92	38.16	0.9729	786,432	0	0.33	52.90	0.9990	262,144	0
Couple	10.66	37.85	0.9489	786,432	0	0.33	52.90	0.9982	262,144	0
Mandril	10.62	37.87	0.9659	786,432	0	0.33	52.92	0.9989	262,144	0
Airplane	11.15	37.66	0.8885	786,432	0	0.33	52.90	0.9958	262,144	0
Average	10.62	37.87	0.9345	786,432	0	0.33	52.91	0.9976	262,144	0

Table 6 Results of Wu and Tsai's [16] and Khodai and Faez's [24] technique

Image size (512×512)	MSE	PSNR	SSIM	Capacity	FOBP	MSE	PSNR	SSIM	Capacity	FOBP
Aerial	9.87	38.19	0.9831	432,440	266	17.12	35.83	0.9604	800,841	246
Lena	5.20	40.97	0.9755	409,776	0	12.98	37.03	0.9299	791,734	0
Cameraman	6.13	40.26	0.9653	407,985	199	12.15	37.32	0.9211	792,441	38
Woman2	3.26	43.00	0.9682	396,090	215	9.02	38.61	0.9165	787,112	227
Pirate	6.51	39.99	0.9784	416,278	1	13.55	36.85	0.9454	793,534	0
Woman	7.38	39.45	0.9767	418,656	1243	33.31	32.94	0.9299	794,845	403
Bridge	12.09	37.31	0.9825	446,619	814	19.22	35.33	0.9661	803,283	478
Couple	7.59	39.33	0.9811	421,905	174	14.978	36.41	0.9513	796,233	51
Mandril	6.84	39.78	0.9871	429,113	4	13.43	36.89	0.9677	796,051	0
Airplane	4.08	42.03	0.9604	397,912	1	9.78	38.26	0.9044	788,200	0
Average	6.90	40.03	0.9758	417,677	292	15.55	36.55	0.9393	794,427	144

Table 7 Results of Mielikainen's [15] LSB matching technique

Image size (512×512)	MSE	PSNR	SSIM	Capacity	FOBP
Aerial	0.37	52.42	0.9984	262,144	0
Lena	0.37	52.43	0.9970	262,144	0
Cameraman	0.37	52.43	0.9963	262,144	0
Woman2	0.37	52.43	0.9961	262,144	0
Pirate	0.37	52.43	0.9977	262,144	0
Woman	0.37	52.43	0.9975	262,144	0
Bridge	0.37	52.50	0.9990	262,144	0
Couple	0.38	52.41	0.9981	262,144	0
Mandril	0.37	52.43	0.9988	262,144	0
Airplane	0.37	52.42	0.9955	262,144	0
Average	0.37	52.43	0.9974	262,144	0

Table 8 Results of Lu et al.'s [43] technique

Image size (512×512)	MSE(1)	MSE(2)	PSNR(1)	PSNR(2)	SSIM(1)	SSIM(2)	Capacity	FOBP(1)	FOBP(2)
Aerial	0.78	0.69	49.24	49.79	0.9972	0.9975	524,288	0	0
Lena	0.78	0.68	49.26	49.81	0.9947	0.9953	524,288	0	0
Cameraman	0.78	0.69	49.26	49.80	0.9933	0.9941	524,288	0	0
Woman2	0.78	0.68	49.25	49.80	0.9930	0.9939	524,288	0	0
Pirate	0.78	0.69	49.27	49.78	0.9959	0.9964	524,288	0	0
Woman	0.77	0.69	49.29	49.80	0.9956	0.9961	524,288	0	0
Bridge	0.76	0.69	49.36	49.75	0.9982	0.9984	524,288	0	0
Couple	0.77	0.69	49.28	49.79	0.9966	0.9970	524,288	0	0
Mandril	0.78	0.69	49.27	49.79	0.9978	0.9980	524,288	0	0
Airplane	0.78	0.69	49.29	49.80	0.9919	0.9929	524,288	0	0
Average	0.77	0.69	49.28	49.79	0.9954	0.9960	524,288	0	0

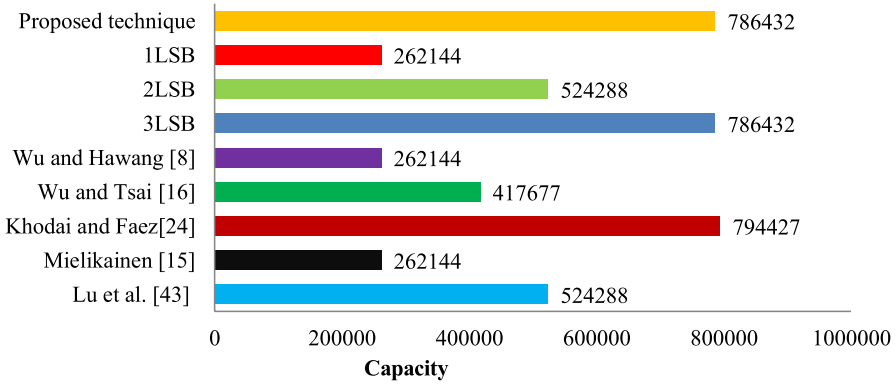


Fig. 8 Comparison of capacity between the proposed and other techniques

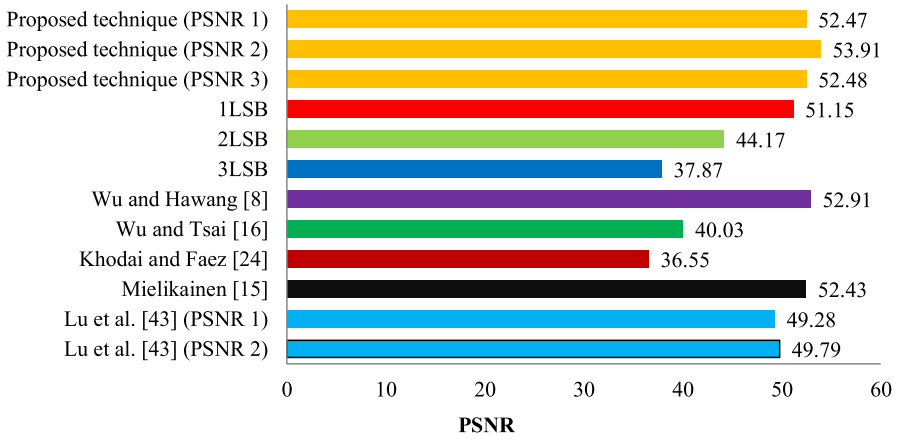


Fig. 9 Comparison of PSNR between the proposed and other techniques

regular group (R_M and R_{-M}) and (2) the singular group (S_M and S_{-M}). For a group of pixels in a block $B=(c_i, c_{i+1} \ldots c_{i+n})$, the smoothness of the groups is measured using the discrimination function $f(c_i, c_{i+1} \ldots c_{i+n}) = \sum_{i=1}^{n-1} |c_{i+1} - c_n|$. Further, two opposite transformation functions, F_1 (transforms even to odd pixel) and F_{-1} (transforms odd to even pixel) are used to count the respective blocks. Then, the groups R_M,R_{-M}, S_M and S_{-M} are obtained using Eqs. (17), (18), (19) and (20).

$$R_M = \frac{\text{Total number of blocks satisfying f}\left(F_1(B)\right) > f(B)}{\text{Total number of blocks}} \tag{17}$$

$$S_M = \frac{\text{Total number of blocks satisfying f}\left(F_1(B)\right) < f(B)}{\text{Total number of blocks}} \tag{18}$$

$$R_{-M} = \frac{\text{Total number of blocks satisfying f}\left(F_{-1}(B)\right) > f(B)}{\text{Total number of blocks}} \tag{19}$$

$$S_{-M} = \frac{\text{Total number of blocks satisfying f}\left(F_{-1}(B)\right) < f(B)}{\text{Total number of blocks}} \tag{20}$$

The RS-plot can be obtained by considering the capacity at the x-axis and regular and singular groups at the y-axis. From the plot in Fig. 10 a,b,c, if we observe the number of regular pixel groups R_M and R_{-M} are almost identical and it is greater than that of the singular groups S_M and S_{-M}, i.e., $R_M \approx R_{-M} > S_M \approx S_{-M}$. So, it can be claimed that the suggested technique is secure to RS-attack. As opposed to this, in Fig. 11 a,b,c the condition $R_{-M} - S_{-M} > R_M - S_M$ exposes the LSB substitution techniques.

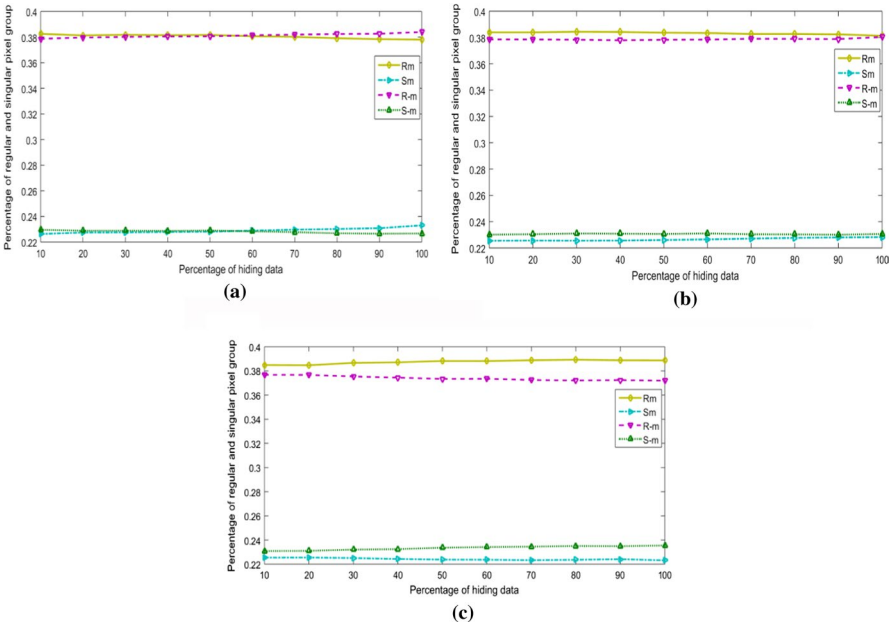


Fig. 10 RS-plots of the proposed technique for Lena **a** SI(1), **b** SI(2) and **c** SI(3)

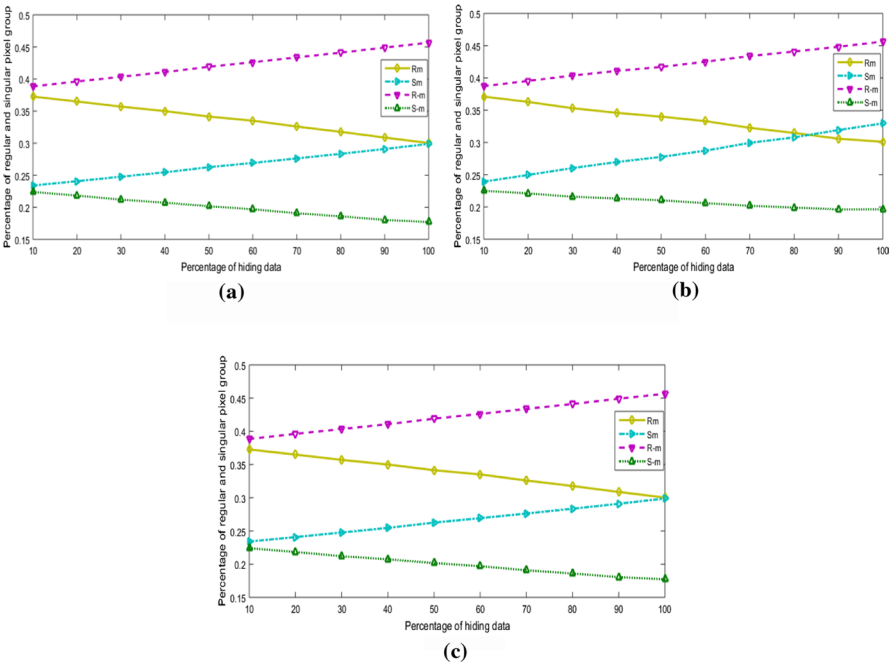


Fig. 11 RS-plots of Lena for a 1LSB, **b** 2LSB and **c** 3LSB

5.1.2 ASA Against PDH Analysis

This section explains the ASA against PDH analysis for the proposed, Wu and Tsai's [16] technique, and Khodai and Faez's [24] technique. To perform PDH analysis, it first finds the FVs between the consecutive pixels of the CI and then finds the same for the SI [58, 59]. As the pixel range lies between 0 to 255, the difference between the two CI pixels can also range from -255 to 255. When we obtain the plot by considering the frequency of the difference values in y-axis and only the difference values in the x-axis for both CI and SI, then the PDH plot can be obtained. Again,

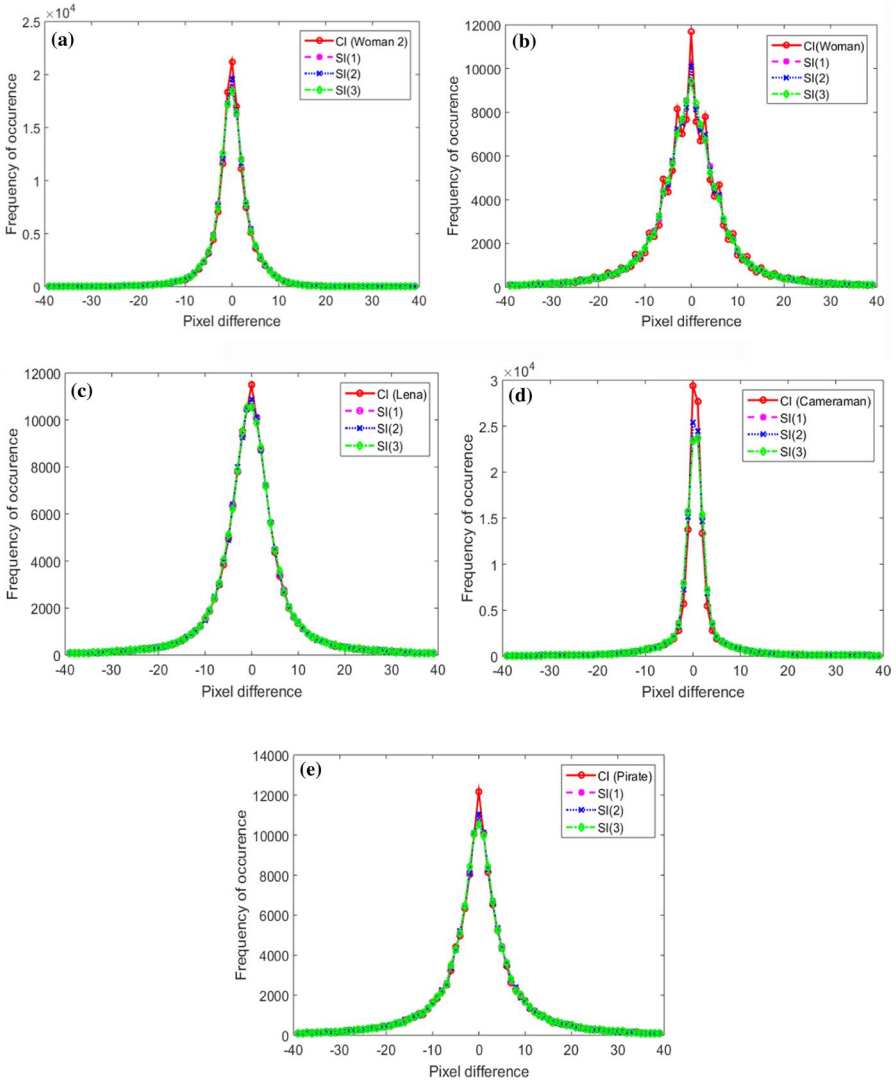


Fig. 12 PDH-plot of the proposed technique for **a** Woman 2, **b** Woman **c** Lena **d** Cameraman and **e** Pirate

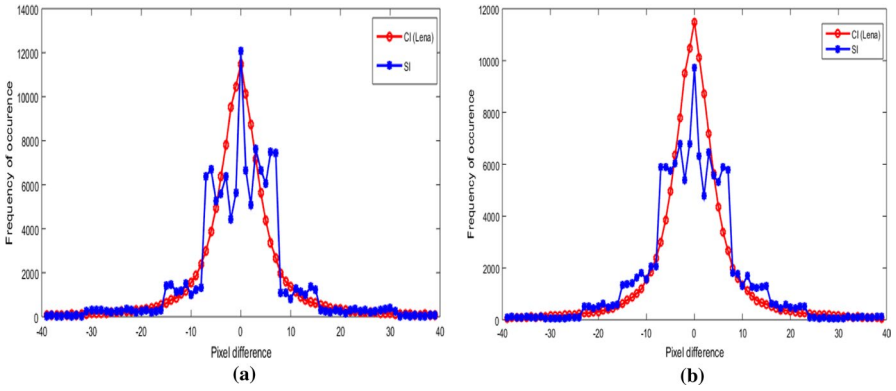


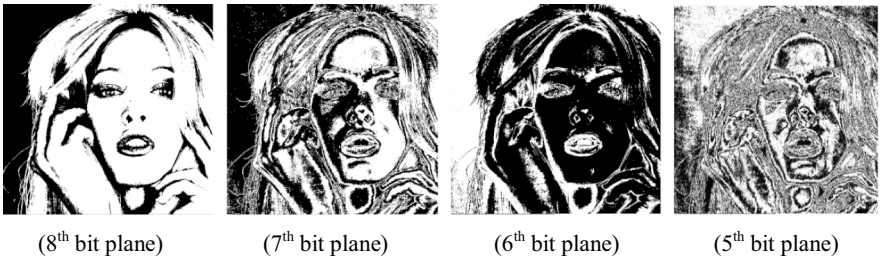
Fig. 13 PDH-plot for Lena for **a** Wu and Tsai's [16] technique and **b** Khodai and Faez's [24] technique

if the plots for the cover and stego-images are identical and merged then it can be concluded that the PDH analysis could not expose the presence of secret information. On the contrary, if the plots for the SI exhibits random, zig-zag nature or makes a good distance from the CI plot then this is an indication of the presence of secret information inside the image. Figure 12a,b,c,d shows the PDH-plots for the proposed technique. From the obtained plot, if we observe the curves for both the cover and stego-images are alike and almost overlapped to each other. Therefore, the presence of secret information is not revealed.

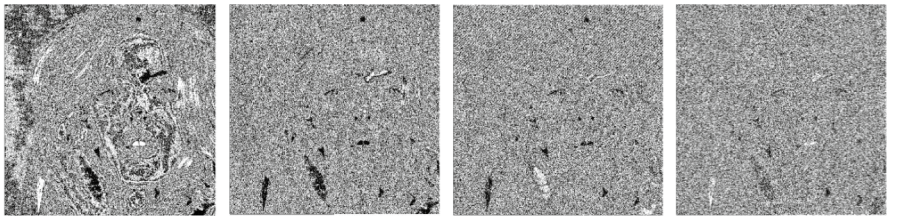
So it can be concluded that the proposed technique shown good resistance to PDH analysis. At the same time, if the observed the PDH-plots for Wu and Tsai's [16] and Khodai and Faez's [24] technique it shows step effects for the SI curve. It is shown in Fig. 13a,b. Therefore, both the two techniques are exposed to PDH analysis.

5.1.3 ASA Against Bit Pair Analysis

Bit plane analysis generally identifies the presence of secret data from the LSBs of the SI pixels. When we compare the bit planes of the LSBs of the CI with the SIs then the modification to the SI can be captured. Figures 14, 15, 16 and 17 show the individual bit planes of the CI and the respective SIs. It can be observed that the bit planes of the CI and the respective SIs are almost identical and therefore, they don't give any visual identification marks. Therefore, the proposed technique is secure to bit plane analysis.

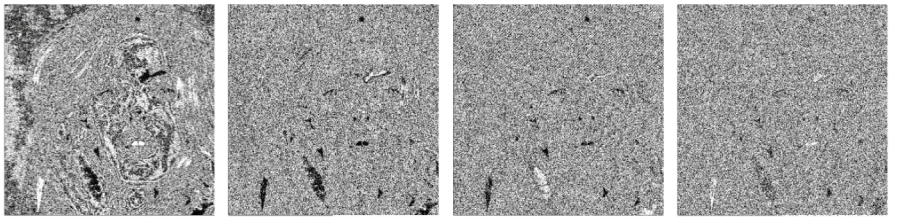


(8th bit plane) (7th bit plane) (6th bit plane) (5th bit plane)



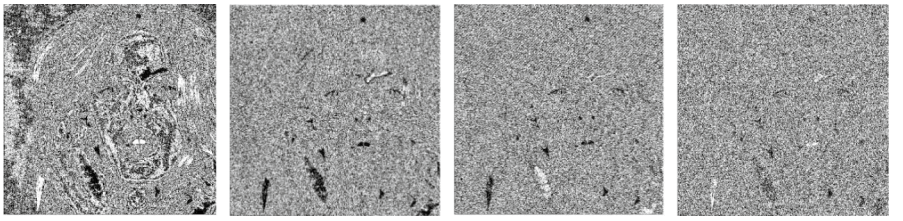
(4th bit plane) (3rd bit plane) (2nd bit plane) (1st bit plane)

Fig. 14 Respective bit planes for the CI



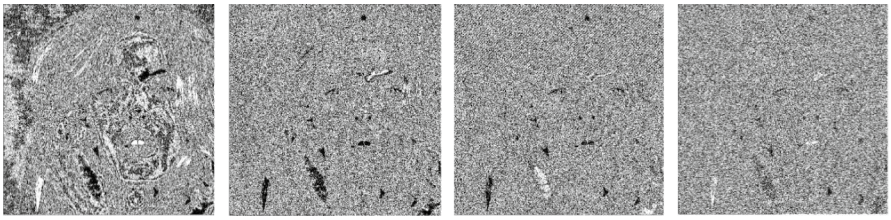
(4th bit plane) (3rd bit plane) (2nd bit plane) (1st bit plane)

Fig. 15 Last four bit planes for the 1st SI



(4th bit plane) (3rd bit plane) (2nd bit plane) (1st bit plane)

Fig. 16 Last four bit planes for the 2nd SI



(4^{th} bit plane) (3^{rd} bit plane) (2^{nd} bit plane) (1^{st} bit plane)

Fig. 17 Last four bit planes for the 3rd SI

6 Conclusion

This paper proposes a shadow image based RDH technique to achieve a fair strike among the conflicting parameters such as capacity, imperceptibility, and security. The shadow image is an identical copy of the CI. The proposed technique produces three shadow images from the CI and the secret bits are embedded in the LSB planes of all the three shadow images. The embedding is performed using the XOR features of the LSB planes and by performing the addition and subtraction logic those planes. The proposed technique observes a maximum of ± 1 modification to the SI pixels. At the receiving end, the CI, as well as the secret bits, are restored successfully. Experimental results indicate the proposed technique outperforms other state-of-art image steganography techniques in terms of capacity and imperceptibility. Further, the proposed technique is resistant to various stego-attacks. Besides, the proposed technique successfully avoids the FOBP. In the future, we aimed to extend this work to further improve the capacity without reducing SI quality. Further, we intend to combine this work with watermarking to achieve authentication.

Funding We declare this work is an independent work and no financial have been received for the work.

Compliance with Ethical Standards

Conflict of interest We declare we have no competing interests.

References

1. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication, 65,* 46–66.
2. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing, 335,* 299–326.
3. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*(2), 142–172.
4. Amirtharajan, R., & Rayappan, J. B. B. (2013). Steganography-time to time: A review. *Research Journal of Information Technology, 5*(2), 53–66.

5. Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. *Computer Science Review, 13,* 95–113.
6. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727–752.
7. Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. *IETE Technical Review, 30*(4), 344–358.
8. Wu, N. I., & Hwang, M. S. (2017). A novel LSB data hiding scheme with the lowest distortion. *The Imaging Science Journal, 65*(6), 371–378.
9. Wang, R. Z., Lin, C. F., & Lin, J. C. (2000). Hiding data in images by optimal moderately-significant-bit replacement. *Electronics Letters, 36*(25), 2069–2070.
10. Chang, C. C., Lin, M. H., & Hu, Y. C. (2002). A fast and secure image hiding scheme based on LSB substitution. *International Journal of Pattern Recognition and Artificial Intelligence, 16*(04), 399–416.
11. Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern recognition, 34*(3), 671–683.
12. Zakaria, A., Hussain, M., Wahab, A., Idris, M., Abdullah, N., & Jung, K. H. (2018). High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. *Applied Sciences, 8*(11), 2199.
13. Yang, H., Sun, X., & Sun, G. (2009). A high-capacity image data hiding scheme using adaptive LSB substitution. *Radioengineering, 18*(4), 509–516.
14. Sharp, T. (2001). An implementation of key-based digital signal steganography. *International workshop on information hiding* (pp. 13–26). Berlin: Springer.
15. Mielikainen, J. (2006). LSB matching revisited. *IEEE Signal Processing Letters, 13*(5), 285–287.
16. Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24*(9–10), 1613–1626.
17. Hameed, M. A., Aly, S., & Hassaballah, M. (2018). An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). *Multimedia Tools and Applications, 77*(12), 14705–14723.
18. Prasad, S., & Pal, A. K. (2017). An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society Open Science, 4*(4), 161066.
19. Jung, K. H., & Yoo, K. Y. (2015). High-capacity index based data hiding method. *Multimedia Tools and Applications, 74*(6), 2179–2193.
20. Liu, H. H., Lin, Y. C., & Lee, C. M. (2019). A digital data hiding scheme based on pixel-value differencing and side match method. *Multimedia Tools and Applications, 78*(9), 12157–12181.
21. Kim, P. H., Yoon, E. J., Ryu, K. W., & Jung, K. H. (2019). Data-hiding scheme using multidirectional pixel-value differencing on colour images. *Security and Communication Networks*. https://doi.org/10.1155/2019/9038650.
22. Wu, H. C., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proceedings-Vision, Image and Signal Processing, 152*(5), 611–615.
23. Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2010). Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. *Journal of Systems and Software, 83*(10), 1635–1643.
24. Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image processing, 6*(6), 677–686.
25. Shukla, A. K., Singh, A., Singh, B., & Kumar, A. (2018). A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing. *IEEE Access, 6,* 51130–51139.
26. Jung, K. H. (2018). Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. *Journal of Real-Time Image Processing, 14*(1), 127–136.
27. Kalita, M., Tuithung, T., & Majumder, S. (2019). An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. *Cryptologia, 43,* 1–24.
28. Liao, X., Wen, Q. Y., & Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. *Journal of Visual Communication and Image Representation, 22*(1), 1–8.
29. Hameed, M. A., Hassaballah, M., Aly, S., & Awad, A. I. (2019). An adaptive image steganography method based on histogram of oriented gradient and PVD–LSB techniques. *IEEE Access, 7,* 185189–185204.

30. Wang, C. M., Wu, N. I., Tsai, C. S., & 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.
31. Joo, J. C., Lee, H. Y., & Lee, H. K. (2010). Improved steganographic method preserving pixel-value differencing histogram with modulus function. *EURASIP Journal on Advances in Signal Processing, 2010*(1), 249826.
32. Maleki, N., Jalali, M., & Jahan, M. V. (2014). Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function. *Egyptian Informatics Journal, 15*(2), 115–127.
33. Sairam, T. D., & Boopathybagan, K. (2019). An improved high capacity data hiding scheme using pixel value adjustment and modulus operation. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-019-7557-9.
34. Shen, S., Huang, L., & Tian, Q. (2015). A novel data hiding for color images based on pixel value difference and modulus function. *Multimedia Tools and Applications, 74*(3), 707–728.
35. Sahu, A. K., & Swain, G. (2019). An optimal information hiding approach based on pixel value differencing and modulus function. *Wireless Personal Communications, 108*(1), 159–174.
36. Liao, X., Wen, Q., & Zhang, J. (2013). Improving the adaptive steganographic methods based on modulus function. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96*(12), 2731–2734.
37. Barton, J. M. (1997). Method and apparatus for embedding authentication information within digital data. *U.S. Patent No. 5,646,997. Washington, DC: U.S. Patent and Trademark Office*.
38. Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE transactions on Circuits and Systems for Video Technology, 13*(8), 890–896.
39. Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing, 13*(8), 1147–1156.
40. Kim, H. J., Sachnev, V., Shi, Y. Q., Nam, J., & Choo, H. G. (2008). A novel difference expansion transform for reversible data embedding. *IEEE Transactions on Information Forensics and Security, 3*(3), 456–465.
41. Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology, 16*(3), 354–362.
42. Tsai, P., Hu, Y. C., & Yeh, H. L. (2009). Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Processing, 89*(6), 1129–1143.
43. Lu, T. C., Tseng, C. Y., & Wu, J. H. (2015). Dual imaging-based reversible hiding technique using LSB matching. *Signal Processing, 108,* 77–89.
44. Lin, J. Y., Chen, Y., Chang, C. C., & Hu, Y. C. (2019). Dual-image-based reversible data hiding scheme with integrity verification using exploiting modification direction. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-019-07783-y.
45. Wang, Y. L., Shen, J. J., & Hwang, M. S. (2017). An Improved Dual Image-based Reversible Hiding Technique Using LSB Matching. *International Journal of Network Security, 19*(5), 858–862.
46. Chang, C. C., Kieu, T. D., & Chou, Y. C. (2007). Reversible data hiding scheme using two steganographic images. In *TENCON 2007–2007 IEEE Region 10 Conference* (pp. 1–4).
47. Sahu, A. K., & Swain, G. (2020). Reversible Image Steganography Using Dual-Layer LSB Matching. *Sensing and Imaging, 21,* 1. https://doi.org/10.1007/s11220-019-0262-y.
48. Kurak, C., & McHugh, J. (1992). A cautionary note on image downgrading. In *Proceedings 8th Annual Computer Security Application Conference* (pp. 153–159).
49. USC-SIPI Image Database. Retrieved 12 December, 2019 http://sipi.usc.edu/database/ database .php?volume=misc.
50. Sahu, A. K., Swain, G., & Babu, E. S. (2018). Digital image steganography using bit flipping. *Cybernetics and Information Technologies, 18*(1), 69–80.
51. Liao, X., Yin, J., Chen, M., & Qin, Z. (2020). Adaptive payload distribution in multiple images steganography based on image texture features. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2020.3004708.
52. Yang, J., & Liao, X. (2020). An embedding strategy on fusing multiple image features for data hiding in multiple images. *Journal of Visual Communication and Image Representation, 71,* 102822.
53. Hassan, F. S., & Gutub, A. (2020). Efficient reversible data hiding multimedia technique based on smart image interpolation. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-020-09513-1.
54. Liao, X., Yu, Y., Li, B., Li, Z., & Qin, Z. (2019). A new payload partition strategy in color image steganography. *IEEE Transactions on Circuits and Systems for Video Technology, 30*(3), 685–696.

55. Hassan, F. S., & Gutub, A. (2020). Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme. *Journal of King Saud University-Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2020.07.
56. Liao, X., Qin, Z., & Ding, L. (2017). Data embedding in digital images using critical functions. *Signal Processing: Image Communication, 58,* 146–156.
57. Fridrich, J., & Goljan, M. (2002). Practical steganalysis of digital images: State of the art. *Security and Watermarking of Multimedia Contents IV, International Society for Optics and Photonics, 4675,* 1–14.
58. Sahu, A. K., & Swain, G. (2019). Dual Stego-imaging based reversible data hiding using improved LSB matching. *International Journal of Intelligent Engineering and Systems, 12*(5), 63–73.
59. Chen, Y. Q., Sun, W. J., Li, L. Y., Chang, C. C., & Wang, X. (2020). An efficient general data hiding scheme based on image interpolation. *Journal of Information Security and Applications, 54,* 102584.