Received: May 13 2019

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Dual Stego-imaging Based Reversible Data Hiding Using Improved LSB Matching

Aditya Kumar Sahu[1,2]* **Gandharba Swain[1]**

[1]*Department of Computer Science and Engineering,*
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh 522502, India
[2]*Department of Computer Science and Engineering,*
GMR Institute of Technology, Rajam, Andhra Pradesh 532127, India
* Corresponding author's Email: adityasahu.cse@gmail.com

Abstract: Since the inception of the reversible data hiding (RDH) concept, it has been a compelling topic in the field of data hiding. Being reversible, it has the ability to restore the original image followed by the successful retrieval of the secret data, at the receiving side. The concept of the dual stego-image based RDH technique utilizes two identical images of the original image for concealing the secret data, has gained wide compliance. Therefore, someone with both the stego-images can only extract the concealed data. In this paper, two improved dual imaging based RDH techniques, such as (1) dual stego-image based pixel pair LSB matching with reversibility, and (2) dual stego-image based modified LSB matching with reversibility, are proposed. In technique 1, at first two mirrored images are obtained from the original image. Then, using the pair of two consecutive pixels from the original image, the mirrored images pixels are modified using LSB matching technique. Later, these pixel pairs are readjusted to ensure reversibility at the receiving side. Similarly, technique 2 utilizes each original pixel to generate two distinct stego-pixels using modified LSB matching. The experimental result shows that the technique 1 maintains excellent peak signal-to-noise ratio (PSNR) of 51.29 dB and 51.30 dB for the two stego-images with hiding capacity (HC) of 524288 bits. At the same time, technique 2 offers 51.19 dB and 49.44 dB of PSNR while exhibiting the equal HC. Further, investigation with various image quality assessment (IQA) metrics like quality index (QI), and structural similarity index (SSIIM) are proven to be competent over the other existing works considered in this paper. In addition, both the proposed techniques have shown excellent anti-steganalytic ability against RS and pixel difference histogram (PDH) attack.

Keywords: Steganography, Reversible data hiding, Hiding capacity, LSB matching.

1. Introduction

Due to the massive development of digitization, the sharing of information becomes convenient [1]. Moreover, features like availability and at a cost next to nothing for the advanced communication devices make this task even easier. However, prevention of classified information from the unauthorized and unqualified interceptors is the major objective of digital data communication [2]. Primarily, cryptography and steganography are the prominent and most effective studies of data hiding field to maintain secrecy while digital content communication [3]. Cryptography, which is used to convert the classified information into an encipher form which cannot be revealed by the attacker. However, the knowledge of data transmission may induce the attacker to divulge the coded information [4]. Another recognized data hiding technique is steganography, where multimedia objects such as image, audio, or video intend to conceal the information inside the respective objects [5-7]. Among them, image steganography has drawn special interest among the researchers. It utilizes the digital images to conceal the secret information and transmits it to the recipient. The image which carries

the embedded information is usually referred as stego-image [8].

Over the years, significant research has been conducted on image steganography. Predominantly, most of them are irreversible, where retrieving the concealed information from the stego-image at the recipient side has been the focal point, but not the original image. Least significant bit (LSB) substitution, pixel value differencing (PVD), exploiting modification direction (EMD), and modulus function are some of the popular irreversible data hiding techniques [9, 10]. However, in some applications, such as law enforcement, military applications, and medical image processing where the loss of a single bit of the original image or the secret data is not tolerable. Research has produced many such image steganography techniques [11, 12] where both retrievals of concealed information, as well as restoration of the complete original image, are possible. Such techniques are regarded as reversible data hiding (RDH) techniques [13]. To the best of our knowledge, the RDH technique [14] has emerged when Barton filed a patent in 1997. Thereafter, RDH techniques have been pivotal among the others in this field.

Recently, dual imaging based RDH techniques has been the point of interest among the steganographers. Most of them employ the concept of LSB matching. Later, Mielikainen's [15] LSB matching technique was one of the well-recognized work in this field which produces high quality stego-image with least possible stego-image distortion. However, Mielikainen's [15] LSB matching technique was irreversible. Lu et al. [16] restored the original image at the receiving side by extending Mielikainen's [15] LSB matching by proposing a rule table. With the use of dual images, the HC for Lu et al.'s [16] technique has been doubled as compared to Mielikainen's [15] technique.

In 2015, Jung [17] has suggested a novel dual image based RDH technique using the concept of the mean and neighboring difference between two consecutive pixels. Actually, they extended the PVD technique using the sub-block strategy to achieve reversibility. It is observed that the suggested technique maintains a good balance between the HC and visual quality.

Generally, RDH techniques are classified into 2 groups, such as (1) Difference expansion (DE) based techniques, and (2) Histogram shifting (HS) based techniques. DE based technique was initially suggested by Tian [18]. Here, the secret bits are concealed using the original difference between the two consecutive pixels and implementing a two-fold expansion technique. However, HC has been sacrificed in the process of achieving reversibility. Later, Alattar [19] modified Tian's technique to improve the HC using four pixels based two-fold expansion technique. Improved and advanced DE based techniques [20, 21] were proposed by many authors. However, these techniques were experienced in limited HC. On the other hand, HS based techniques recognize the peak points of the image and secret bits are concealed in those points. Ni et al. [22], was the first to propose this technique. Tsai et al. [23] improved the HC than Ni et al. [22] by concealing the secret bits in the overlapped pixels between the peak and zero points. Later, Wang et al. [24] proposed multi-layers embedding using the genetic algorithm technique to extend the HC with visually imperceptible stego-image.

The explanation of Lu et al.'s [16] technique is presented in the related section. However, it has been observed that Lu et al.'s [16] technique can be improved with respect to the visual quality while maintaining the exact HC. Therefore, in this paper, two improved dual stego-imaging based RDH techniques applying the concept of LSB matching are proposed.

The major developments of the proposed techniques are outlined below:

(1) Both the proposed RDH techniques adequately conceal the secret bits in two images. Thus, someone without having one of the images could never be able to retrieve the secret bits.

(2) The techniques effectively withstand against RS attack and pixel difference histogram (PDH) attack.

(3) Finally, both the proposed techniques produce high quality stego-images with decent HC.

The remainder of the work is coordinated as follows. Mielikainen's technique [15] and Lu et al.'s technique [16] have been reviewed in the related work section. The proposed RDH techniques are presented in Section 3. Next, the simulation results and comparisons are discussed in Section 4. Finally, closing remarks are given in Section 5.

2. Related work

2.1 Mielikainen's LSB matching revisited technique [15]

The LSB matching revisited technique [15] modifies the original image pixels randomly by ±1. In this, at first two consecutive pixels are chosen for hiding the secret bits. The secret bits are embedded in the original pixels using a binary function (F). The binary function $F(g_1, g_2)$ is of the form as follows :

$$F(g_1,g_2) = LSB(\lfloor g_1 / 2 \rfloor + g_2) \quad (1)$$

Where, g_1 and g_2 are the two consecutive pixels of a block.
Let, s_1 and s_2 be the two secret bits. The stego-pixels (g_1^*, g_2^*) can be obtained using Eq. (2).

$$(g_1^*, g_2^*) = \begin{cases} (g_1, g_2), \text{if } (LSB(g_1) = s_1) \text{ and } (F(g_1, g_2) = s_2) \\ (g_1, g_2 + 1), \text{if } (LSB(g_1) = s_1) \text{ and } (F(g_1, g_2) \neq s_2) \\ (g_1 - 1, g_2), \text{if } (LSB(g_1) \neq s_1) \text{ and } (F(g_1 - 1, g_2) = s_2) \\ (g_1 + 1, g_2), \text{if } (LSB(g_1) \neq s_1) \text{ and } (F(g_1 + 1, g_2) \neq s_2) \end{cases} \quad (2)$$

At the extraction side, the secret bit s_1 can be obtained from the LSB of g_1^* and s_2 can be computed using Eq. (3).

$$s_2 = LSB(\lfloor g_1^* / 2 \rfloor + g_2^*) \quad (3)$$

Consider an example with two original pixels g_1 = 50 and g_2 = 60. Let the secret data be s_1 = 0 and s_2 = 1. From Eq. (2), the condition $LSB(50) = 0$ and $F(50,60) = 1$ is satisfied. Therefore, the two stego-pixels are g_1^* = 50 and g_2^* = 60. At the receiver side, the secret bit s_1 can be found using $LSB(g_1^*) = LSB(50) = 0$. Similarly, the secret bit s_2 can be found using Eq. (3) as $LSB(\lfloor 50 / 2 \rfloor + 60) = 1$.

2.2 Lu et al.'s [16] dual imaging based RDH approach

Lu et al. [16] extended Mielikainen's [15] technique using two identical images of the original image to restore the original image pixels with the secret data at the receiver side. At first, two identical images from the original image are obtained. Then, using [15] the secret bits are embedded. Further, the pixels after embedding are readjusted using the suggested modification table to ensure the original pixels can be restored at the receiver side. An illustration demonstrating Lu et al.'s [16] technique is presented below.

Assume the two original pixels are o_1 = 30, o_2 = 32. Let the secret bits to be embedded are 0010_2. The two identical pixels obtained from the original pixels are m_1 = 30, m_2 = 32 and g_1 = 30, g_2 = 32. Here, (m_1,m_2) are the pixels of the first identical image. Similarly, (g_1,g_2) are the pixels of second identical image. Firstly, the secret bit 00_2 are embedded in m_1 = 30, m_2 = 32 using Eq. (2). Similarly, the bits 10_2 are embedded in g_1 = 30, g_2 = 32. After embedding the secret bits, the new pixels are m_1' = 30, m_2' = 33 and g_1' = 29, g_2' = 32. Now, utilizing the pixel modification rule table, the pixels are readjusted as follows; since, $(m_1' - m_1) = 0$, $(m_2' - m_2) = 1$, $(g_1' - g_1) = -1$, $(g_2' - g_2) = 0$, now using the rule table the stego-pixels are readjusted as $m_1^* = m_1 + 2 = 32$, $m_2^* = m_2 = 32$, $g_1^* = g_1 - 1 = 29$, $g_2^* = g_2 = 32$. At the receiver side, from the LSB of the stego-pixel m_1^* the bit 0_2 and using Eq (3) for m_1^* and m_2^* the bit 0_2 are obtained. Similarly, from the LSB of the stego-pixel g_1^* the bit 1_2 and using Eq.(3) for g_1^* and g_2^* the bit 0_2 are obtained. Finally, the original pixels can be restored using the averaging strategy from the stego-pixels as, $o_1 = \lfloor (m_1^* + g_1^*)/2 \rfloor = \lfloor (32 + 29)/2 \rfloor = 30$ and $o_2 = \lfloor (m_2^* + g_2^*)/2 \rfloor = \lfloor (32+32)/2 \rfloor = 32$.

3. Proposed work

In this section, both the two proposed techniques are discussed. Consider the original image O with pixels $\{o_1,o_2,o_3,o_4,\ldots..,o_n\}$ and its two mirrored images are M and G with pixels $(m_1,m_2,m_3,m_4,\ldots.,m_n\}$ and $(g_1,g_2,g_3,g_4,\ldots..,g_n)$ respectively. The mirrored images are the replica of the original image. The technique 1 called as dual stego-image based pixel pair LSB matching with reversibility, initially considers a pair of two consecutive pixels (o_1,o_2) from the original image. Then, using the LSB matching [15] two separate pairs (m_1, m_2) and (g_1, g_2) for the mirrored images are modified. Each pair of the two mirrored image hides 2 bits. Later, the pixels are readjusted to ensure it can be restored at the receiver side with exact data recovery. Similarly, the techniques 2 called as dual stego-image based modified LSB matching with reversibility. Here, applying modified LSB matching, two distinct stego-pixels are obtained for each original pixel. Later, with these two separate sets of stego-pixels, two stego-images are obtained. Further, Fig. 1 illustrates the embedding, extraction, and pixel restoration process for the proposed dual stego-image based pixel pair LSB matching with reversibility technique. Fig. 2 illustrates the proposed dual stego-image based modified LSB matching with reversibility technique. The manifestations of the embedding and extraction algorithm for the proposed techniques are narrated in subsection 3.1 and 3.2.

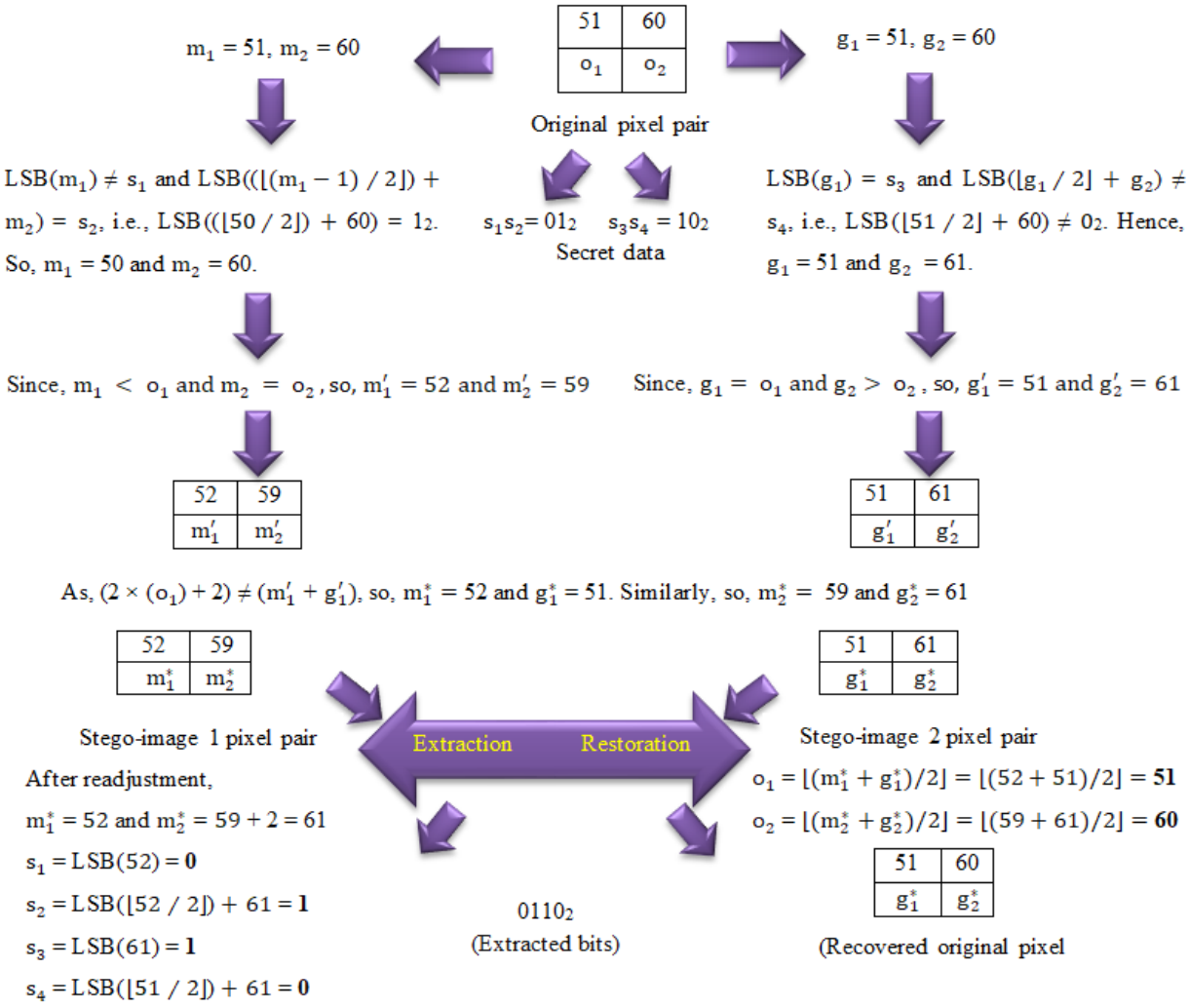


Figure. 1 An illustration of embedding, extraction, and pixel restoration process for the proposed dual stego-image based pixel pair LSB matching with reversibility technique

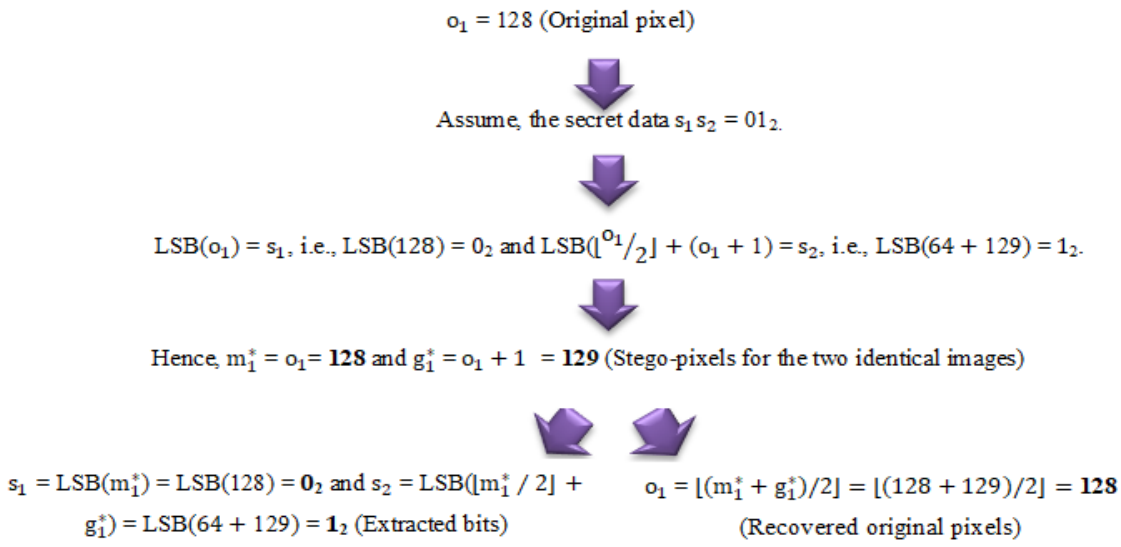


Fig. 2 An illustration of the embedding, extraction, and pixel restoration process for the proposed dual image based modified LSB matching with reversibility technique

3.1 Technique 1: Dual stego-image based pixel pair LSB matching with reversibility

The embedding, pixel extraction, and restoration algorithm for this technique are presented below.

3.1.1. Embedding algorithm

Step 1: Initially, using the original pixel pair (o_1,o_2) and two secret bits s_1s_2 modify the pixel pair (m_1, m_2) for the first mirrored image M using Eq. (4).

$$(m_1, m_2) = \begin{cases} (m_1, m_2), \text{if } (\text{LSB}(o_1) = s_1) \text{ and } (\text{avg}_1 = s_2) \\ (m_1, m_2 + 1), \text{if } (\text{LSB}(o_1) = s_1) \text{ and} (\text{avg}_1 \neq s_2) \\ (m_1 - 1, m_2), \text{if } (\text{LSB}(o_1) \neq s_1) \text{ and } (\text{avg}_2 = s_2) \\ (m_1 + 1, m_2), \text{if } (\text{LSB}(o_1) \neq s_1) \text{ and } (\text{avg}_2 \neq s_2) \end{cases} \quad (4)$$

Where $\text{avg}_1 = \text{LSB}\left(\left\lfloor {}^{o_1}/_{2}\right\rfloor + o_2\right)$ and $\text{avg}_2 = \text{LSB}\left(\left\lfloor {}^{(o_1 - 1)}/_{2}\right\rfloor + o_2\right)$.

Similarly, obtain the pixel pair (g_1, g_2) for the second mirrored image G using (o_1,o_2) and the next two secret bits s_3s_4 using Eq. (4).

Step 2: Now, obtain the readjusted pixel pairs (m_1', m_2') and (g_1', g_2') using Eqs. (5) and (6).

$$(m_1', m_2') = \begin{cases} (m_1 + 2, m_2 - 1), \text{if } m_1 < o_1 \text{ and } m_2 = o_2 \\ (m_1, m_2), \text{otherwise} \end{cases} \quad (5)$$

$$(g_1', g_2') = \begin{cases} (g_1 + 2, g_2 - 1), \text{if } g_1 < o_1 \text{ and } g_2 = o_2 \\ (g_1, g_2), \text{otherwise} \end{cases} \quad (6)$$

Step 3: Finally, observe Eq. (7) to obtain the stego-pixels m_1^* and g_1^*.

$$(m_{1,}^* g_1^*) = \begin{cases} (m_1' - 2, g_1') \text{ if } \left((2 \times o_1) + 2\right) = m_1' + g_1' \\ (m_1', g_1'), \text{otherwise} \end{cases} \quad (7)$$

Similarly, assign the values of m_2' to m_2^*, and g_2' to g_2^*. Then, readjust the stego-pixels m_2^* and g_2^* as follows:

If $(2 \times o_2) > (m_2' + g_2')$ and $m_2' \geq g_2'$
  then $g_2^* = g_2' + 2$
else $m_2^* = m_2' + 2$
else if $\left((2 \times o_2) + 2\right) = m_2' + g_2'$
  then $m_2^* = m_2' - 2$

Step 4: Embedding is done.

3.1.2. Pixel restoration and extraction algorithm

Step 1: At the receiving side, the original pixel pair (o_1,o_2) can be recovered using Eq. (8).

$$o_1 = \lfloor (m_1^* + g_1^*)/2 \rfloor, \; o_2 = \lfloor (m_2^* + g_2^*)/2 \rfloor \quad (8)$$

Step 2: Now, to extract the secret bits, the stego-pixel pair (m_1^*, m_2^*) are readjusted using Eqs. (9) and (10).

$$m_1^* = \begin{cases} m_1^* + 2, \text{if } m_1^* + 2 = g_1^* \\ m_1^*, \text{otherwise} \end{cases} \quad (9)$$

$$m_2^* = \begin{cases} m_2^* + 2, \text{if } m_2^* + 2 = g_2^* \\ m_2^*, \text{otherwise} \end{cases} \quad (10)$$

Step 3: Finally, obtain the secret bit s_1 and s_3 from the LSB of m_1^* and m_2^*. Similarly, the secret bit s_2 and s_4 can be retrieved using Eq. (11).

$$s_2 = \text{LSB}(\lfloor m_1^* / 2 \rfloor + m_2^*), \; s_4 = \text{LSB}(\lfloor g_1^* / 2 \rfloor + g_2^*) \quad (11)$$

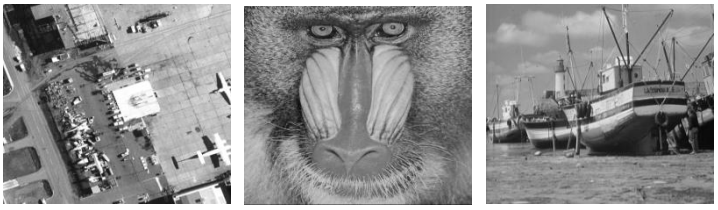
Step 4: Extraction is done.

3.2 Technique 2: Dual stego-image based modified LSB matching with reversibility

3.2.1. Embedding, extraction, and pixel restoration algorithm

Step 1: Assume the original image O consists of pixels $\{\mathbf{o_1},\mathbf{o_2},\mathbf{o_3},\mathbf{o_4},\ldots,\mathbf{o_n}\}$. In this section, the embedding procedure for one of the original pixel $\mathbf{o_1}$ is demonstrated.

Step 2: Now, using the original image pixel o_1 and two secret bits s_1s_2, obtain the sego-pixels (m_1^*, g_1^*) using Eq. (12).



(a) (b) (c)

Figure. 3 Original images: (a) airfield, (b) baboon, and (c) boat

$$(m_1^*, g_1^*) = \begin{cases} (o_1, o_1 + 1), \text{if } (\text{LSB}(o_1) = s_1) \text{ and } (\text{avg}_3 = s_2) \\ (o_1, o_1), \text{if } (\text{LSB}(o_1) = s_1) \text{ and } (\text{avg}_3 \neq s_2) \\ (o_1 - 1, o_1 + 1), \text{if } (\text{LSB}(o_1) \neq s_1) \text{ and } (\text{avg}_4 = s_2) \\ (o_1 + 1, o_1 - 1), \text{if } (\text{LSB}(o_1) \neq s_1) \text{ and } (\text{avg}_4 \neq s_2) \end{cases} \quad (12)$$

Where $\text{avg}_3 = \text{LSB}\left(\left\lfloor {}^{o_1}/_{2} \right\rfloor + (o_1 + 1)\right)$ and $\text{avg}_4 = \text{LSB}\left(\left\lfloor {}^{(o_1 - 1)}/_{2} \right\rfloor + (o_1 + 1)\right)$.

Step 3: Now, repeat step 2 for each original pixel to the end pixel o_n and obtain the two different stego-images M^* and G^* consisting of pixels $(m_1^*, m_2^*, m_3^*, m_4^*, \ldots, m_n^*)$ and $(g_1^*, g_2^*, g_3^*, g_4^*, \ldots, g_n^*)$.

Step 4: Embedding is done.

Step 5: At the extraction side, the secret bit s_1 can be directly retrieved by obtaining the LSB of m_1^*. Similarly, s_2 can be retrieved using Eq. (13).

$$s_2 = \text{LSB}(\lfloor m_1^* / 2 \rfloor + g_1^*) \quad (13)$$

Step 6: Apply Eq. (14) to recover the original image pixel o_1.

$$o_1 = \lfloor (m_1^* + (g_1^*))/2 \rfloor \quad (14)$$

4. Simulation results and comparisons

The simulation was conducted using MATLAB R(2015a) software on the windows platform. The hardware configurations consist of Processor Intel(R) Core(TM) i5-8250U CPU@1.60GHz 1.80GHz, and RAM 4.0GB. The original images with size 512 × 512 pixels were selected from USC–SIPI image databases [25] and some of them are shown in Fig. 3.

Since Mielikainen's [15] and Lu et al.'s [16] technique utilizes LSB matching strategy to embed the secret data; therefore both of them were considered for comparison purpose. Further, Jung's [17] reversible technique performs the embedding on dual images using PVD sub-block technique, hence this technique also considered. The comparison with respect to the peak signal-to-noise ratio (PSNR), hiding capacity (HC), quality index (QI), and structural similarity index (SSIM) are performed to show the superiority of the proposed technique. PSNR is used to measure the distortion between the original and the stego-images. It should be at the higher side for visually indistinguishable images. Eq. (15) computes the PSNR. It is measured in terms of decibel (dB).

$$\text{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{m \times n} \Sigma_{i=1}^{m} \Sigma_{j=1}^{n} (p_{ij} - q_{ij})^2} \quad (15)$$

Where, p_{ij} and q_{ij} are the pixels at position (i, j) of the original and stego-images respectively.

The HC is the maximum number of embedding bits in the stego-image. QI measures the similarity between the original and stego-image. The highest value for QI is 1. This can be achieved when both the original and stego-images are completely identical. QI can be computed using Eq. (16).

$$\text{QI} = \frac{4 \sigma_{xy} \bar{p}\bar{q}}{(\sigma_x^2 + \sigma_y^2)\,[(\bar{p})^2 + (\bar{q})^2]} \quad (16)$$

Where $\bar{p}$ and σ_x are the mean of pixels and standard deviation for the original image. Similarly, $\bar{q}$ and σ_y are the mean of pixels and standard deviation for stego-image. σ_{xy} is the covariance between the original and stego-images.

The SSIM index measures the quality of the stego-image. SSIM value close to 1 produces better quality of stego-image [26]. The SSIM can be computed using Eq. (17).

$$\text{SSIM} = \frac{(2\bar{p}\bar{q} + c_1)(2\sigma_{pq} + c_2)}{(\bar{p}^2 + \bar{q}^2 + c_1)(\sigma_p^2 + \sigma_q^2 + c_2)} \quad (17)$$

Where $\bar{p}$, $\bar{p}^2$, σ_p^2 and $\bar{q}$, $\bar{q}^2$, σ_q^2 are the mean pixel values, variance and the standard deviation for the original image and stego-image respectively. Similarly, $2\sigma_{pq}$ is the covariance between the original and stego-image. c_1 and c_2 are the constants, where $c_1 = k_1 L$ and $c_2 = k_2 L$ and $k_1 = 0.01$, $k_2 = 0.03$ and L is 255.

The PSNR and HC for Mielikainen's [15], Lu et al.'s [16], Jung's [17], and the proposed techniques are presented in Tables 1 and 2. The PSNR for the two stego-images are represented as PSNR 1 and PSNR 2. In case of the proposed technique 1, both the PSNR 1 and 2 are 51.29 dB and 51.30 dB Which is larger compared to Lu et al.'s [16] technique and Jung's [17] technique with equal HC. Similarly, for the proposed technique 2, the PSNR 1 is 51.19 dB and PSNR 2 is 49.44 dB. The PSNR 1 of the technique 2 is larger compared to Lu et al.'s [16] and Jung's [17] techniques PSNR 1, whereas the PSNR 2 is almost equal with Lu et al.'s technique. However, the average PSNR for Mielikainen's technique [15] is slightly larger compared to both techniques, but the HC for the proposed techniques are doubled than Mielikainen's technique [15]. Further, the QI for both the stego-images QI(1) and QI(2) for both the proposed techniques are competent compared to the existing techniques. Similarly, the SSIM for both the proposed technique is found to be superior with 0.9982 and 0.9988 for technique 1, and 0.9977 and 0.9973 for technique 2, respectively

4.1 Security analysis

In this section, the security of the proposed techniques against (1) RS steganalysis, and (2) Pixel difference histogram (PDH) steganalysis are evaluated and presented.

4.1.1. Analysis against RS attack

The RS analysis is conducted to show the attack resistance of the proposed technique. To perform the RS analysis, initially, the pixels are classified into three groups, such as (i) the regular group with R_M and R_{-M}, (ii) singular group with S_M and S_{-M}, and (iii) the unusable group [27, 28]. The discrimination function (DF) is used to find the magnitude of the respective pixel blocks for parameters R_M, R_{-M}, S_M and S_{-M}. The x-axis of the RS plot represents the percentage of EC and the y-axis represents the percentage of regular or singular groups. The condition $R_M \approx R_{-M} > S_M \approx S_{-M}$ suggests the approach successfully resists to RS attack. On the contrary, the condition $R_{-M} - S_{-M} > R_M - S_M$

Table 1. Results for the proposed technique 1

Image 512×512	HC	PSNR (1)	PSNR (2)	QI(1)	QI(2)	SSIM(1)	SSIM(2)
Airfield	524288	51.34	51.38	0.9970	0.9980	0.9983	0.9989
Baboon	524288	51.26	51.28	0.9984	0.9990	0.9987	0.9992
Boat	524288	51.26	51.26	0.9933	0.9957	0.9972	0.9982
Bridge	524288	51.33	51.34	0.9984	0.9989	0.9987	0.9991
Couple	524288	51.26	51.27	0.9948	0.9967	0.9974	0.9984
House	524288	51.26	51.27	0.9928	0.9954	0.9973	0.9983
Houses	524288	51.30	51.31	0.9954	0.9971	0.9985	0.9990
Lena	524288	51.27	51.26	0.9865	0.9913	0.9994	0.9990
Average	**524288**	**51.29**	**51.30**	**0.9946**	**0.9965**	**0.9982**	**0.9988**

Table 2. Results for the proposed technique 2

Image 512×512	HC	PSNR (1)	PSNR (2)	QI(1)	QI(2)	SSIM(1)	SSIM(2)
Airfield	524288	51.24	49.50	0.9969	0.9961	0.9983	0.9977
Baboon	524288	51.16	49.41	0.9983	0.9977	0.9987	0.9982
Boat	524288	51.18	49.41	0.9933	0.9908	0.9971	0.9992
Bridge	524288	51.21	49.5	0.9983	0.9977	0.9986	0.9980
Couple	524288	51.18	49.42	0.9948	0.9929	0.9974	0.9964
House	524288	51.18	49.42	0.9927	0.9901	0.9972	0.9962
Houses	524288	51.22	49.46	0.9954	0.9938	0.9985	0.9979
Lena	524288	51.17	49.41	0.9863	0.9814	0.9960	0.9945
Average	**524288**	**51.19**	**49.44**	**0.9945**	**0.9926**	**0.9977**	**0.9973**

Table 3. Results for Mielikainen [15], and Lu et al. [16]

Image 512×512	Mielikainen [15]				Lu et al. [16]						
	HC	PSNR	QI	SSIM	HC	PSNR (1)	PSNR (2)	QI(1)	QI(2)	SSIM(1)	SSIM(2)
Airfield	262144	52.42	0.9977	0.9979	524288	49.28	49.81	0.9951	0.9953	0.9972	0.9976
Baboon	262144	52.41	0.9988	0.9991	524288	49.27	49.79	0.9969	0.9973	0.9983	0.9985
Boat	262144	52.43	0.9951	0.9979	524288	49.31	49.82	0.9911	0.9922	0.9962	0.9967
Bridge	262144	52.42	0.9988	0.9987	524288	49.27	49.79	0.9954	0.9965	0.9998	0.9998
Couple	262144	52.43	0.9963	0.9978	524288	49.27	49.79	0.9941	0.9943	0.9982	0.9981
House	262144	52.44	0.9947	0.998	524288	49.29	49.81	0.9905	0.9914	0.9963	0.9968
Houses	262144	52.45	0.9967	0.9989	524288	49.28	49.81	0.994	0.9947	0.998	0.9982
Lena	262144	52.42	0.9901	0.997	524288	49.27	49.84	0.9821	0.9841	0.9947	0.9953
Average	**262144**	**52.43**	**0.9960**	**0.9982**	**524288**	**49.28**	**49.81**	**0.9924**	**0.9932**	**0.9973**	**0.9976**

Table 4. Results for Jung [17]

Image 512×512	HC	PSNR (1)	PSNR (2)	QI(1)	QI(2)	SSIM(1)	SSIM(2)
Airfield	650221	35.16	34.18	0.9871	0.9844	0.9880	0.9859
Baboon	701792	34.76	34.25	0.9894	0.9879	0.9887	0.9869
Boat	519039	37.44	36.79	0.9875	0.9835	0.9906	0.9886
Bridge	684567	36.84	35.49	0.9898	0.9884	0.9895	0.9883
Couple	516867	37.99	37.39	0.9882	0.9848	0.9906	0.9889
House	474892	40.06	39.18	0.9907	0.9867	0.9922	0.9902
Houses	663200	33.2	32.04	0.9866	0.9831	0.9882	0.9861
Lena	436564	39.34	38.57	0.9891	0.9814	0.9922	0.9896
Average	**580893**	**36.85**	**35.99**	**0.9886**	**0.9850**	**0.9900**	**0.9881**

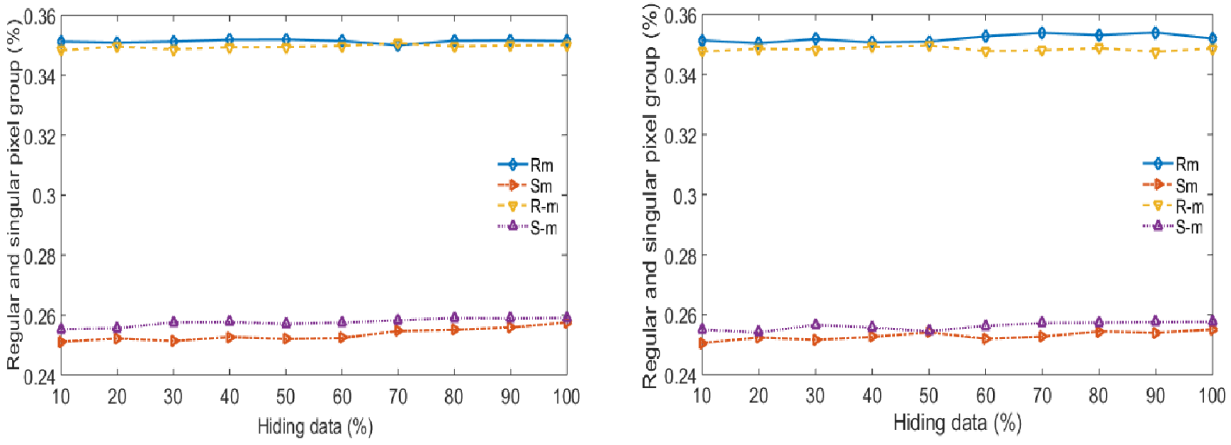
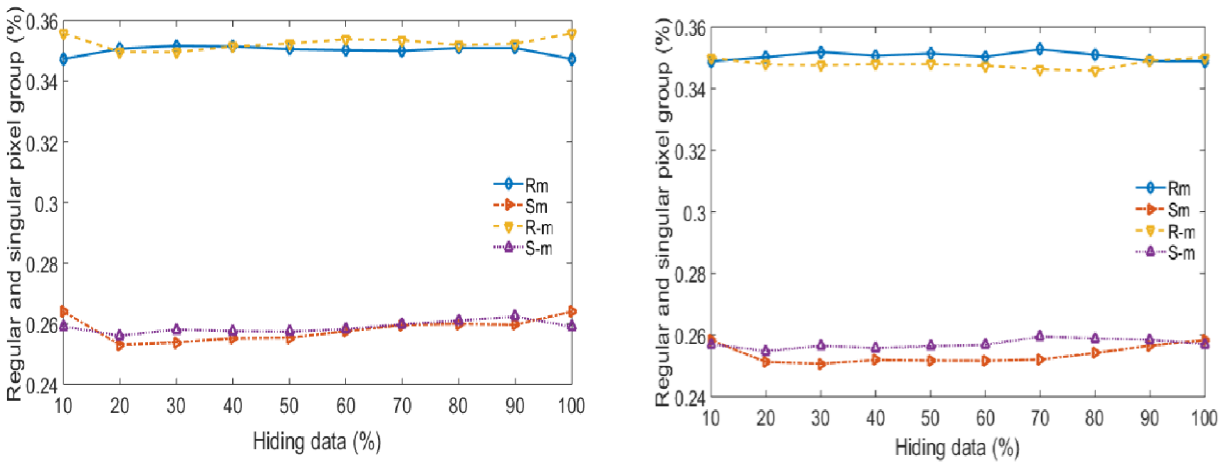


Figure.4 RS plot for the proposed dual stego-image based pixel pair LSB matching with reversibility for: (a) boat SI 1 and (b) boat SI 2

exposes the approach against the RS attack. Fig 4 and 5 shows the RS plot for the Boat image for both the techniques. This can be clearly observed from the obtained RS curve that the condition $R_M \approx R_{-M} > S_M \approx S_{-M}$ is satisfying for all the images. So both the proposed techniques are proven to be undetected by RS analysis.

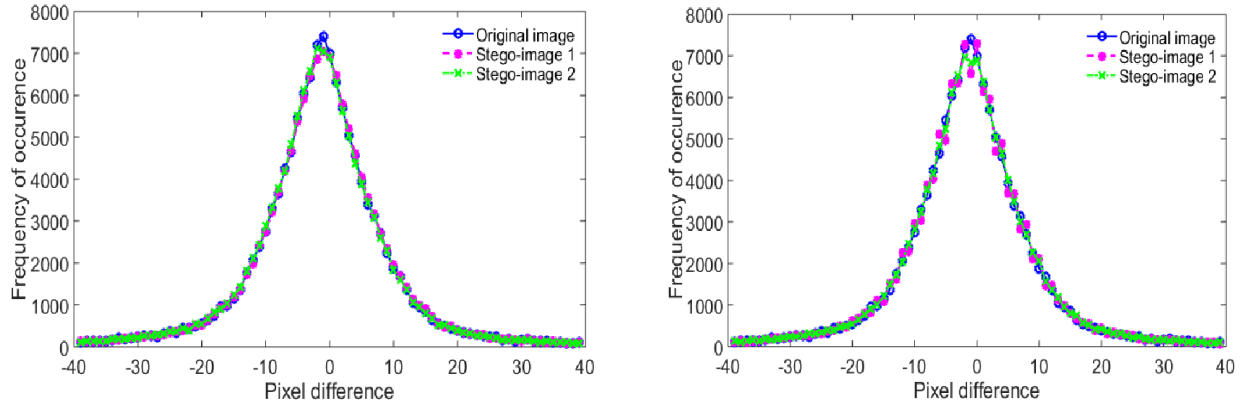
4.1.2. Pixel difference histogram (PDH) steganalysis

In the case of a grayscale image, the difference between two consecutive pixels ranges from 255 to 255 [29-31]. The PDH plot for the original image



(a) (b)

Figure. 5 RS plot for the dual stego-image based modified LSB matching with reversibility technique for: (a) Boat SI 1 and (b) boat SI 2



(a) (b)

Figure. 6 PDH plots of the Boat Image for: (a) technique 1 and (b) technique 2

can be drawn by obtaining the difference between two consecutive pixels in the x-axis and the corresponding frequency of the difference values on the y-axis. The PDH plots for the original images are usually smooth with no zig-zag appearance or step-effects. Then, the PDH plot for the stego-images is found. If we notice the zig-zag nature in the case of stego-image plots then we can say that the method is exposed to PDH analysis. The PDH plots for the proposed technique for the Boat image are presented in Fig. 6. It is noticeable that the respective PDH plots for the original and its corresponding stego-images are overlapped with each other. Further, there are no step-effects for the stego-images are noticed. Therefore, the proposed techniques successfully resist PDH analysis.

5. Conclusion

In this paper, two improved RDH techniques to increase the hiding capacity (HC) without reducing image quality are proposed. Initially, two mirrored images are obtained from the original image in technique 1. Then, applying LSB matching technique to the pair of two consecutive original pixels, the mirrored images pixels are readjusted for concealing the secret data. Similarly, in the case of technique 2, from each original pixel, two different stego-pixels are obtained. Both the techniques ensure complete reversibility of the original image and extraction of secret data at the recipient end. The technique 1 offers PSNR of 51.29 dB, and 51.30 dB, respectively for both the stego-images with HC of 524288 bits. Similarly, technique 2 offers 51.19 dB and 49.44 dB of PSNR while maintaining the equal HC. Further, QI, and SSIM metrics are also acceptable. In addition, both the proposed techniques showed exceptional ability to combat against RS and PDH analysis.

In the future, applying the theory of image interpolation, the HC can be improved without

sacrificing the image quality. Further, using field-programmable gate array (FPGA), we intend to extend the work for real-time applications.

Acknowledgments

We declare this work is an independent work and no financial assistance has been received for the work.

References

[1] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey", *Signal Processing: Image Communication*, Vol. 65, pp. 46-66, 2018.

[2] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels", *Journal of Visual Communication and Image Representation*, Vol. 28, pp. 21-27, 2015

[3] A.K. Sahu and G. Swain, "An Improved Data Hiding Technique Using Bit Differencing and LSB Matching", *Internetworking Indonesia Journal*, Vol. 10, No.1, pp. 17-21, 2018.

[4] A.K. Sahu and G. Swain, "A Review on LSB Substitution and PVD Based Image Steganography Techniques", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 2, No. 3, pp. 712-719, 2016.

[5] M. Hussain, A. W. A. Wahab, N. Javed, and K. H Jung, "Recursive information hiding scheme through LSB, PVD shift, and MPE", *IETE Technical Review*, Vol. 35, No. 1, pp. 53-63, 2018.

[6] A.K. Sahu and G. Swain, "An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function", *Wireless Personal Communications*, pp. 1-16, 2019.

[7] A.K. Sahu and G. Swain, "A Novel Multi Stego-image based Data Hiding Method for Gray Scale Image", *Pertanika Journal of Science & Technology*, Vol. 27, No. 2, pp. 753-768, 2019.

[8] A.K. Sahu, G. Swain, and E. S Babu "Digital Image Steganography Using Bit Flipping", *Cybernetics and Information Technologies*, Vol. 18, No. 1, pp. 69-80, 2018.

[9] M. A. Hameed, S. Aly, and M. Hassaballah, "An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD)", *Multimedia Tools and Applications*, Vol. 77, No. 12, pp. 14705–14723, 2017.

[10] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters*, Vol. 24, No. 9-10, 1613-1626, 2003.

[11] C. Chang, Y. C. Chou, and T. D. Kieu, "Information hiding in dual images with reversibility", In: *Proc. of Third International Conference on Multimedia and Ubiquitous Engineering*, pp. 145-152, 2009,

[12] F. Jafar, K. A. Darabkh, R. T. Al-Zubi, and R. R. Saifan, "An efficient reversible data hiding algorithm using two steganographic images", *Signal Processing*, Vol. 128, pp. 98-109, 2016.

[13] F. Di, M. Zhang, X. Liao, and J. Liu, "High-fidelity reversible data hiding by Quadtree-based pixel value ordering", *Multimedia Tools and Applications*, pp. 1-17, 2018

[14] J. M. Barton, "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*, 1997.

[15] J. Mielikainen, "LSB matching revisited", *IEEE Signal Processing Letters*, Vol. 13, No. 5, pp. 285-287, 2006.

[16] T. C. Lu, C. Y. Tseng, and J. H. Wu, "Dual imaging-based reversible hiding technique using LSB matching", *Signal Processing*, Vol. 108, pp. 77-89, 2015.

[17] K. H. Jung, "Dual image based reversible data hiding method using neighbouring pixel value differencing", *The Imaging Science Journal*, Vol. 63, No. 7, pp. 398-407, 2015.

[18] J. Tian, "Reversible data embedding using a difference expansion", *IEEE transactions on Circuits and Systems for Video Technology*, Vol.13, No. 8, pp. 890-896, 2003.

[19] A.M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", *IEEE Transactions on Image Processing*, Vol. 13, No. 8, pp. 1147-1156, 2004

[20] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding", *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3, pp. 456-465, 2008.

[21] W. He, G. Xiong, S. Weng, Z. Cai, and Y. Wang, "Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion", *Information Sciences*, Vol. 467, pp. 784-799, 2018.

[22] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding", *IEEE Transactions*

on Circuits and Systems for Video Technology, Vol. 16, No. 3, 354-362, 2006.
[23] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting", *Signal Processing*, Vol. 89, No. 6, 1129-1143, 2009.
[24] J. Wang, J. Ni, X. Zhang, and Y. Q. Shi, "Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting", *IEEE transactions on Cybernetics*, Vol. 47, No. 2, 315-326, 2017.
[25] USC-SIPI Image Database. [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc. Accessed 19 Feb, 2019.
[26] A.K. Sahu and G. Swain, "A Novel n-Rightmost Bit Replacement Image Steganography Technique", *3D Research*, Vol. 10, No. 2, 2019.
[27] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges", *Multimedia Tools and Applications*, Vol. 75, No. 21, pp. 13541-13556, 2016.
[28] A.K. Sahu and G. Swain, "Pixel Overlapping Image Steganography Using PVD and Modulus Function", *3D Research*, Vol. 9, No. 40, 2018.
[29] A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, "Performance evaluation parameters of image steganography techniques", In: *Proc. of International Conference on Research Advances in Integrated Navigation Systems*, pp. 1-8, 2016.
[30] A.K. Sahu and G. Swain, "Information hiding using group of bits substitution", *International Journal on Communications Antenna and Propagation*, Vol. 7, No. 2, pp.162-167, 2017.
[31] A.K. Sahu and M. Sahu, "Digital image steganography techniques in spatial domain: a study", *International Journal of Pharmacy & Technology*, Vol. 8, No. 4, pp.5205-5217, 2016.