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

Aditya Kumar Sahu¹²* Gandharba Swain¹

¹Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh 522502, India
²Department 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 (SSIM) 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:

$\text{International Journal of Intelligent Engineering and Systems, Vol.12, No.5, 2019} \quad \text{DOI: 10.22266/ijies2019.1031.07}$
\[
F(g_1, g_2) = \text{LSB}(\lfloor g_1/2 \rfloor + g_2)
\]  
(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).

\[
(g_1^*, g_2^*) = \begin{cases} 
(g_1, g_2), & \text{if } (\text{LSB}(g_1) = s_1) \text{ and } (F(g_1, g_2) = s_2) \\
(g_1 + 1, g_2), & \text{if } (\text{LSB}(g_1) = s_1) \text{ and } (F(g_1, g_2) \neq s_2) \\
(g_1 - 1, g_2), & \text{if } (\text{LSB}(g_1) \neq s_1) \text{ and } (F(g_1 - 1, g_2) = s_2) \\
(g_1 + 1, g_2), & \text{if } (\text{LSB}(g_1) \neq s_1) \text{ and } (F(g_1 + 1, g_2) \neq s_2)
\end{cases}
\]  
(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).

\[
s_2 = \text{LSB}(\lfloor g_1^*/2 \rfloor + g_2^*)
\]  
(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 \(\text{LSB}(50) = 0\) and \(F(50, 60) = 1\) is satisfied. Therefore, the two stego-pixels \(g_1^* = 50\) and \(g_2^* = 60\). At the receiver side, the secret bit \(s_1\) can be found using LSB\((g_1^*) = \text{LSB}(50) = 0\). 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 00102. 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 are embedded in \(m_1 = 30, m_2 = 32\) using Eq. (2).

Similarly, the bits 10 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 02 and using Eq. (3) for \(m_1^*\) and \(m_2^*\) the bit 02 are obtained. Similarly, from the LSB of the stego-pixel \(g_1^*\) the bit 12 and using Eq. (3) for \(g_1^*\) and \(g_2^*\) the bit 02 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.

\[
\begin{align*}
\text{Original pixel pair} & \quad \text{Secret data} \\
\begin{array}{c}
51 \\
01 \\
102
\end{array} & \quad \begin{array}{c}
60 \\
o_1 \\
o_2
\end{array} \\
\text{LSB}(m_1) = s_1 \text{ and } \text{LSB}([((m_1 - 1) / 2) + m_2]) = s_2, \text{ i.e., } \text{LSB}([51 / 2]) + 60 = 12. \\
\text{So, } m_1 = 50 \text{ and } m_2 = 60.
\end{align*}
\]

\[
\text{Since, } m_1 < o_1 \text{ and } m_2 = o_2, \text{ so, } m'_1 = 52 \text{ and } m'_2 = 59.
\]

\[
\begin{align*}
\text{Stego-image 1 pixel pair} & \quad \text{After readjustment,} \\
\begin{array}{c}
52 \\
m'_1
\end{array} & \quad \begin{array}{c}
59 \\
m'_2
\end{array} \\
\text{As, } (2 \times (c_1) + 2) \neq (m'_1 + g'_1), \text{ so, } m'_1 = 52 \text{ and } g'_1 = 51. \text{ Similarly, so, } m'_2 = 59 \text{ and } g'_2 = 61.
\end{align*}
\]

\[
\begin{align*}
\text{Stego-image 2 pixel pair} & \quad \begin{array}{c}
51 \\
g'_1
\end{array} & \quad \begin{array}{c}
61 \\
g'_2
\end{array}
\end{align*}
\]

\[
\text{Extraction} \\
\text{Restoration}
\]

\[
\begin{align*}
o_1 &= 128 \text{ (Original pixel)} \\
\text{Assume, the secret data } s_1, s_2 = 01_2,
\end{align*}
\]

\[
\begin{align*}
\text{LSB}(o_1) = s_1, \text{ i.e., } \text{LSB}(128) = 0_2 \text{ and } \text{LSB}([o_1 / 2]) + (o_1 + 1) = s_2, \text{ i.e., } \text{LSB}(64 + 129) = 1_2.
\end{align*}
\]

\[
\text{Hence, } m'_1 = o_1 = 128 \text{ and } g'_1 = o_1 + 1 = 129 \text{ (Stego pixels for the two identical images)}
\]

\[
\begin{align*}
\text{Recovered original pixels} \\
\begin{array}{c}
41 \\
\bar{g}_1
\end{array} & \quad \begin{array}{c}
60 \\
\bar{g}_2
\end{array}
\end{align*}
\]

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

\[
\begin{align*}
s_1 &= \text{LSB}(m'_1) = \text{LSB}(128) = 0_2 \text{ and } s_2 = \text{LSB}([m'_1 / 2]) + \text{LSB}(128) = (41 + 60)/2 = 128 \\
g'_1 &= \text{LSB}(64 + 129) = 1_2 \text{ (Extracted bits)} \quad \text{Recovered original pixels}
\end{align*}
\]
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).

\[
\begin{align*}
(m_1, m_2) &= \\
&= \begin{cases} 
(m_1, m_2), & \text{if } (\text{LSB}(o_1) = s_1) \text{ and } (\text{avg}_1 = s_2) \\
(m_1, m_2 + 1), & \text{if } (\text{LSB}(o_1) = s_1) \text{ and } (\text{avg}_1 \neq s_2) \\
(m_1 - 1, m_2), & \text{if } (\text{LSB}(o_1) \neq s_1) \text{ and } (\text{avg}_2 = s_2) \\
(m_1 + 1, m_2), & \text{if } (\text{LSB}(o_1) \neq s_1) \text{ and } (\text{avg}_2 \neq s_2)
\end{cases}
\end{align*}
\]

Where \(\text{avg}_1 = \text{LSB}([\text{avg}_1/2] + o_2)\) and \(\text{avg}_2 = \text{LSB}([\text{avg}_1/2] + o_2)\).

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).

\[
\begin{align*}
(m'_1, m'_2) &= \\
&= \begin{cases} 
(m_1 + 2, m_2 - 1), & \text{if } m_1 < o_1 \text{ and } m_2 = o_2 \\
(m_1, m_2), & \text{otherwise}
\end{cases}
\end{align*}
\]

\[
\begin{align*}
(g'_1, g'_2) &= \\
&= \begin{cases} 
(g_1 + 2, g_2 - 1), & \text{if } g_1 < o_1 \text{ and } g_2 = o_2 \\
g_1, g_2), & \text{otherwise}
\end{cases}
\end{align*}
\]

Step 3: Finally, observe Eq. (7) to obtain the stego-pixels \(m'_1\) and \(g'_1\).

\[
\begin{align*}
(m'_1, g'_1) &= \\
&= \begin{cases} 
(m'_1 - 2, g'_1), & \text{if } (2 \times o_1) + 2 = m'_1 + g'_1 \\
(m'_1, g'_1), & \text{otherwise}
\end{cases}
\end{align*}
\]

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:

\[
\begin{align*}
\text{If } (2 \times o_2) > (m'_2 + g'_2) \text{ and } m'_2 \geq g'_2 & \text{ then } g'_2 = g'_2 + 2 \\
\text{else } m'_2 = m'_2 + 2 & \text{ else if } ((2 \times o_2) + 2) = m'_2 + g'_2 \\
& \text{ then } m'_2 = m'_2 - 2
\end{align*}
\]

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).

\[
o_1 = [(m'_1 + g'_1)/2], o_2 = [(m'_2 + g'_2)/2]
\]

Step 2: Now, to extract the secret bits, the stego-pixel pair \((m'_1, m'_2)\) are readjusted using Eqs. (9) and (10).

\[
\begin{align*}
m'_1 &= \begin{cases} 
m'_1 + 2, & \text{if } m'_1 + 2 = g'_1 \\
m'_1, & \text{otherwise}
\end{cases}
\end{align*}
\]

\[
\begin{align*}
m'_2 &= \begin{cases} 
m'_2 + 2, & \text{if } m'_2 + 2 = g'_2 \\
m'_2, & \text{otherwise}
\end{cases}
\end{align*}
\]

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).

\[
s_2 = \text{LSB}([m'_1 / 2] + m'_2), s_4 = \text{LSB}([g'_1 / 2] + g'_2)
\]

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 \(\{o_1, o_2, o_3, o_4, \ldots, o_n\}\). In this section, the embedding procedure for one of the original pixel \(o_1\) is demonstrated.

Step 2: Now, using the original image pixel \(o_1\) and two secret bits \(s_1s_2\), obtain the stego-pixels \((m'_1, g'_1)\) using Eq. (12).
$\text{(m}_1, \text{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}
$ (12)

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

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 $(m_1^1, m_2^1, m_3^1, m_4^1, \ldots, m_n^1)$ and $(g_1^1, g_2^1, g_3^1, g_4^1, \ldots, g_n^1)$.

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 $m_1^1$. Similarly, $s_2$ can be retrieved using Eq. (13).

$$s_2 = \text{LSB}\left(\left\lfloor \frac{m_1^1}{2} \right\rfloor + g_1^1 \right)$$ (13)

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

$$o_1 = \left(\frac{(m_1^1 + g_1^1)}{2}\right)$$ (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 $512 \times 512$ pixels were selected from USC–SIPI image databases [25] and some of them are shown in Fig. 3.

Since Mieliainen'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).

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

$$\text{QI} = \frac{4 \sigma_{xy} p q}{\sigma_p^2 + \sigma_q^2 + \sigma_{xy}^2} \left[ \frac{1}{2} \right]$$ (16)

Where $\bar{p}$ and $\sigma_p$ are the mean of pixels and standard deviation for the original image. Similarly, $\bar{q}$ and $\sigma_q$ are the mean of pixels and standard deviation for stego-image. $\sigma_{xy}$ 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).

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

Where $\bar{p}, \bar{q}, \sigma_p^2$ and $\bar{q}, \bar{q}^2, \sigma_q^2$ 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 $c_1 = k_1L$ and $c_2 = k_2L$ 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>
<thead>
<tr>
<th>Image 512x512</th>
<th>HC</th>
<th>PSNR (1)</th>
<th>PSNR (2)</th>
<th>QI(1)</th>
<th>QI(2)</th>
<th>SSIM(1)</th>
<th>SSIM(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airfield</td>
<td>524288</td>
<td>51.34</td>
<td>51.38</td>
<td>0.9970</td>
<td>0.9980</td>
<td>0.9983</td>
<td>0.9989</td>
</tr>
<tr>
<td>Baboon</td>
<td>524288</td>
<td>51.26</td>
<td>51.28</td>
<td>0.9984</td>
<td>0.9990</td>
<td>0.9987</td>
<td>0.9992</td>
</tr>
<tr>
<td>Boat</td>
<td>524288</td>
<td>51.26</td>
<td>51.26</td>
<td>0.9933</td>
<td>0.9957</td>
<td>0.9972</td>
<td>0.9982</td>
</tr>
<tr>
<td>Bridge</td>
<td>524288</td>
<td>51.33</td>
<td>51.34</td>
<td>0.9984</td>
<td>0.9989</td>
<td>0.9987</td>
<td>0.9991</td>
</tr>
<tr>
<td>Couple</td>
<td>524288</td>
<td>51.26</td>
<td>51.27</td>
<td>0.9948</td>
<td>0.9967</td>
<td>0.9974</td>
<td>0.9984</td>
</tr>
<tr>
<td>House</td>
<td>524288</td>
<td>51.26</td>
<td>51.27</td>
<td>0.9928</td>
<td>0.9954</td>
<td>0.9973</td>
<td>0.9983</td>
</tr>
<tr>
<td>Houses</td>
<td>524288</td>
<td>51.30</td>
<td>51.31</td>
<td>0.9954</td>
<td>0.9971</td>
<td>0.9985</td>
<td>0.9990</td>
</tr>
<tr>
<td>Lena</td>
<td>524288</td>
<td>51.27</td>
<td>51.26</td>
<td>0.9865</td>
<td>0.9913</td>
<td>0.9994</td>
<td>0.9990</td>
</tr>
<tr>
<td>Average</td>
<td>524288</td>
<td>51.29</td>
<td>51.30</td>
<td>0.9946</td>
<td>0.9965</td>
<td>0.9982</td>
<td>0.9988</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Image 512x512</th>
<th>HC</th>
<th>PSNR (1)</th>
<th>PSNR (2)</th>
<th>QI(1)</th>
<th>QI(2)</th>
<th>SSIM(1)</th>
<th>SSIM(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airfield</td>
<td>524288</td>
<td>51.24</td>
<td>49.50</td>
<td>0.9969</td>
<td>0.9961</td>
<td>0.9983</td>
<td>0.9977</td>
</tr>
<tr>
<td>Baboon</td>
<td>524288</td>
<td>51.16</td>
<td>49.41</td>
<td>0.9983</td>
<td>0.9977</td>
<td>0.9987</td>
<td>0.9982</td>
</tr>
<tr>
<td>Boat</td>
<td>524288</td>
<td>51.18</td>
<td>49.41</td>
<td>0.9933</td>
<td>0.9908</td>
<td>0.9971</td>
<td>0.9992</td>
</tr>
<tr>
<td>Bridge</td>
<td>524288</td>
<td>51.21</td>
<td>49.5</td>
<td>0.9983</td>
<td>0.9977</td>
<td>0.9986</td>
<td>0.9980</td>
</tr>
<tr>
<td>Couple</td>
<td>524288</td>
<td>51.18</td>
<td>49.42</td>
<td>0.9948</td>
<td>0.9929</td>
<td>0.9974</td>
<td>0.9964</td>
</tr>
<tr>
<td>House</td>
<td>524288</td>
<td>51.18</td>
<td>49.42</td>
<td>0.9927</td>
<td>0.9901</td>
<td>0.9972</td>
<td>0.9962</td>
</tr>
<tr>
<td>Houses</td>
<td>524288</td>
<td>51.22</td>
<td>49.46</td>
<td>0.9954</td>
<td>0.9938</td>
<td>0.9985</td>
<td>0.9979</td>
</tr>
<tr>
<td>Lena</td>
<td>524288</td>
<td>51.17</td>
<td>49.41</td>
<td>0.9863</td>
<td>0.9814</td>
<td>0.9960</td>
<td>0.9945</td>
</tr>
<tr>
<td>Average</td>
<td>524288</td>
<td>51.19</td>
<td>49.44</td>
<td>0.9945</td>
<td>0.9926</td>
<td>0.9977</td>
<td>0.9973</td>
</tr>
</tbody>
</table>
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

---

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

<table>
<thead>
<tr>
<th>Image 512x512</th>
<th>Mielikainen [15]</th>
<th>Lu et al. [16]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HC</td>
<td>PSNR</td>
</tr>
<tr>
<td>Airfield</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baboon</td>
<td>262144</td>
<td>52.42</td>
</tr>
<tr>
<td>Boat</td>
<td>262144</td>
<td>52.51</td>
</tr>
<tr>
<td>Bridge</td>
<td>262144</td>
<td>52.42</td>
</tr>
<tr>
<td>Couple</td>
<td>262144</td>
<td>52.43</td>
</tr>
<tr>
<td>House</td>
<td>262144</td>
<td>52.44</td>
</tr>
<tr>
<td>Houses</td>
<td>262144</td>
<td>52.45</td>
</tr>
<tr>
<td>Lena</td>
<td>262144</td>
<td>52.42</td>
</tr>
<tr>
<td>Average</td>
<td>262144</td>
<td>52.43</td>
</tr>
</tbody>
</table>

**Table 4. Results for Jung [17]**

<table>
<thead>
<tr>
<th>Image 512x512</th>
<th>HC</th>
<th>PSNR (1)</th>
<th>PSNR (2)</th>
<th>QI(1)</th>
<th>QI(2)</th>
<th>SSIM(1)</th>
<th>SSIM(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airfield</td>
<td>650221</td>
<td>35.16</td>
<td>34.18</td>
<td>0.9871</td>
<td>0.9844</td>
<td>0.9880</td>
<td>0.9859</td>
</tr>
<tr>
<td>Baboon</td>
<td>701792</td>
<td>34.76</td>
<td>34.25</td>
<td>0.9894</td>
<td>0.9879</td>
<td>0.9887</td>
<td>0.9869</td>
</tr>
<tr>
<td>Boat</td>
<td>519039</td>
<td>37.44</td>
<td>36.79</td>
<td>0.9875</td>
<td>0.9835</td>
<td>0.9906</td>
<td>0.9886</td>
</tr>
<tr>
<td>Bridge</td>
<td>684567</td>
<td>36.84</td>
<td>35.49</td>
<td>0.9898</td>
<td>0.9884</td>
<td>0.9895</td>
<td>0.9883</td>
</tr>
<tr>
<td>Couple</td>
<td>516867</td>
<td>37.99</td>
<td>37.39</td>
<td>0.9882</td>
<td>0.9848</td>
<td>0.9906</td>
<td>0.9889</td>
</tr>
<tr>
<td>House</td>
<td>474982</td>
<td>40.06</td>
<td>39.18</td>
<td>0.9907</td>
<td>0.9867</td>
<td>0.9922</td>
<td>0.9902</td>
</tr>
<tr>
<td>Houses</td>
<td>663200</td>
<td>33.2</td>
<td>32.04</td>
<td>0.9866</td>
<td>0.9831</td>
<td>0.9882</td>
<td>0.9861</td>
</tr>
<tr>
<td>Lena</td>
<td>436564</td>
<td>39.34</td>
<td>38.57</td>
<td>0.9891</td>
<td>0.9814</td>
<td>0.9922</td>
<td>0.9896</td>
</tr>
<tr>
<td>Average</td>
<td>580893</td>
<td>36.85</td>
<td>35.99</td>
<td>0.9886</td>
<td>0.9850</td>
<td>0.9900</td>
<td>0.9881</td>
</tr>
</tbody>
</table>

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
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


