Signal Processing: Image Communication 101 (2022) 116556

Contents lists available at ScienceDirect

Signal Processing: Image Communication

journal homepage: www.elsevier.com/locate/image

A reversible modified least significant bit (LSB) matching revisited method

Hsien-Wen Tseng [a,*], Hui-Shih Leng [b]

[a] Department of Information Management, Chaoyang University of Technology, Taichung 41349, Taiwan
[b] Department of Mathematics, National Changhua University of Education, Changhua 50058, Taiwan

ARTICLE INFO

Keywords:
LSB matching
EMD
Dual images reversible data hiding

ABSTRACT

Least Significant Bit (LSB) matching revisited method is a modification to the LSB matching, which is a data hiding method for embedding message bits into a cover image. The modified method achieves the same hiding payload as LSB matching, but with fewer changes to the cover image. According to the embedding algorithm, we found that the LSB matching revisited method can be viewed as a kind of Exploiting Modification Direction (EMD) method. By using the modified LSB matching method and EMD, a simple dual images Reversible Data Hiding (RDH) method is proposed. The experimental results show that the proposed method achieves better image quality and hiding capacity. The image quality is evaluated using Peak Signal Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Moreover, Regular and Singular (RS) analysis reveals that the proposed method is secure against Steganalysis.

1. Introduction

Data hiding is a technique that embeds secret message into cover images. It is used to prevent illegal users from stealing the secret message during transmission. After embedding, the cover images are transformed to stego images with little distortion. Thus nobody knows the secret message is embedded in the stego images. The transmission of the stego images will not attract the attentions of illegal users on the Internet, and to protect of the secret message.

Least significant bit (LSB) replacement method is a simple and popular data hiding scheme proposed by Turner [1]. The method directly substitutes k secret bits into k least significant bits of each cover pixel. LSB matching method [2] also modifies the LSBs of the cover image for message embedding. If the message bit does not match the LSB of the cover image pixel, the pixel value is randomly either added or subtracted by one. Thus the LSB matching method is also named ± 1 embedding. Mielikainen [3] proposed a modified LSB matching method in 2006, a pair of pixels as a group is used for embedding, where the LSB of the first pixel carries one secret message bit, and a binary function carries another secret message bit. After embedding, only one pixel in the pair is either added or subtracted by one. As a result, the change to the pixel values is little, and the image distortion is reduced.

There are some methods [4,5] that perform data hiding based on the LSB matching method. Recently dual images based reversible data hiding (RDH) [6–16] are proposed where dual copies of a cover image are used to embed the secret data. Reversible data hiding (RDH) referred to as lossless or invertible data hiding. Lu et al. [7] proposed a dual imaging-based reversible hiding technique using LSB matching in 2015. Wang et al. [6] proposed an improved dual image-based reversible hiding technique using LSB matching in 2017. The second pixel of the pixel pair is used to increase the hiding capacity. The technique makes a copy of the cover image, embeds the secret message into the two images using LSB matching method. Besides, Lu et al. [10] also proposed reversible data hiding in dual stego-images using frequency-based encoding strategy in 2017.

In this paper, a reversible data hiding method based on LSB matching revisited method and EMD is proposed to embed the secret message bits in dual images. When we study the LSB matching revisited method, we found that LSB matching revisited method can be viewed as a kind of EMD method (see Section 3.1). This helps us to develop a RDH method based on LSB matching revisited method and EMD. Experimental results show the proposed method improves the stego images quality and preserves the hiding capacity. The major contributions of this work are listed below:

(1) This study shows that LSB matching revisited method is a kind of EMD method.
(2) A simple and novel EMD-based RDH is proposed.
(3) The proposed method improves the stego images quality of EMD-based RDH.

The rest of this paper is organized as follows. In Section 2, the relevant methods of the research are introduced. The proposed method is presented in Section 3. Experimental results and comparisons are given in Section 4. Finally, conclusions are drawn in Section 5.

* Corresponding author.
E-mail addresses: hwtseng@cyut.edu.tw (H.-W. Tseng), lenghs@cc.ncue.edu.tw (H.-S. Leng).

https://doi.org/10.1016/j.image.2021.116556
Received 23 August 2020; Received in revised form 30 August 2021; Accepted 31 October 2021
Available online 16 November 2021

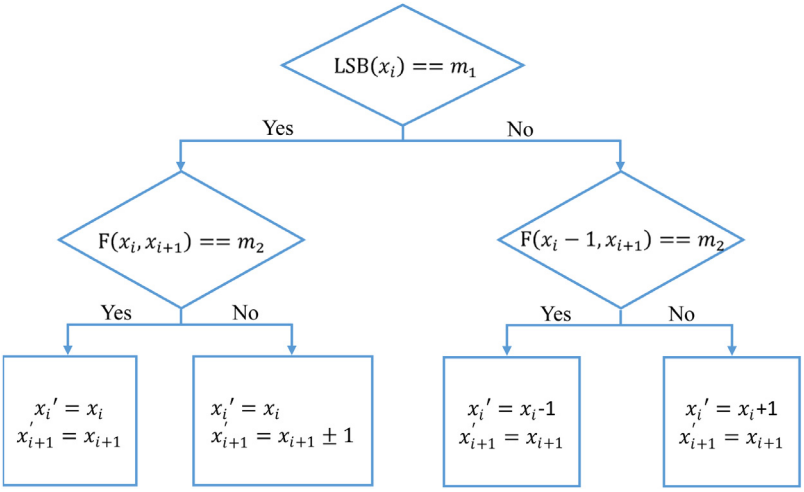

Fig. 1. The flowchart of LSB matching revisited method.

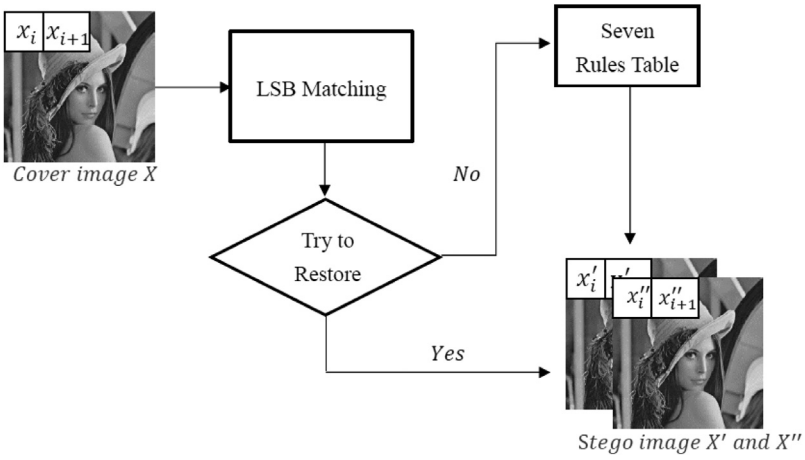

Fig. 2. The flow diagram of Lu et al.'s method.

2. Related works

2.1. LSB matching revisited method

Mielikainen [3] proposed the LSB matching revisited method in 2006. A binary function is used to carry secret message bits. The method takes two pixels as a group, the LSB of the first pixel carries one secret bit, and the binary function carries another secret bit. The embedding process is shown in Fig. 1.

Assume the two pixels are (x_i, x_{i+1}), the two secret message bits are (m_1, m_2). Firstly LSB(x_i) extracts the least significant bit from pixel x_i and determine whether it is equal to the secret bit m_1. If they are equal, and the binary the function $F(x_i, x_{i+1})$ is used to carry the secret bit m_2. If $F(x_i, x_{i+1}) = m_2$, then the stego image pixels $(x_i', x_{i+1}') = (x_i, x_{i+1})$, else $(x_i', x_{i+1}') = (x_i, x_{i+1} \pm 1)$. When $LSB(x_i) \neq m_1$, $F(x_i - 1, x_{i+1})$ is checked to carry the secret bit m_2. If they are equal, let $(x_i', x_{i+1}') = (x_i - 1, x_{i+1})$; else let $(x_i', x_{i+1}') = (x_i + 1, x_{i+1})$. The binary function $F(x_i, x_{i+1})$ is shown as Eq. (1). Additionally the binary function has properties $F(x_i - 1, x_{i+1}) \neq F(x_i + 1, x_{i+1})$ and $F(x_i, x_{i+1}) \neq F(x_i, x_{i+1} + 1)$.

$$F(x_i, x_{i+1}) = LSB(\left\lfloor \frac{x_i}{2} \right\rfloor + x_{i+1}) \tag{1}$$

2.2. Dual-images reversible data hiding techniques using LSB matching method

Lu et al. [7] proposed the dual imaging-based reversible hiding technique using LSB matching method in 2015. Just like the LSB matching revisited method, the method uses two cover image pixels (x_i, x_{i+1}) at a time. Two secret message bits (m_1, m_2) are embedded into the stego image pixels (x_i', x_{i+1}') using the LSB matching revisited method. Then the same two cover image pixels (x_i, x_{i+1}) is used again to embed another two secret message bits (m_3, m_4), and another stego image pixels (x_i'', x_{i+1}'') are created using the LSB matching revisited method. Fig. 2 shows the flow diagram of Lu et al.'s method.

In order to recover the original image pixels, the stego image pixels are checked using Eq. (2). If $y_i = x_i$ and $y_{i+1} = x_{i+1}$, then the original image pixels can be recovered. If not, a seven rules table is used for adjusting the pixel values. The seven rules table is shown in Table 1. There are 7 cases that cannot recover the original pixels. For example, if $(x_i, x_{i+1}) = (37, 33)$ and $(m_1, m_2, m_3, m_4) = (0, 0, 0, 0)$, then the stego image pixels will be $(x_i', x_{i+1}') = (38, 33)$ and $(x_i'', x_{i+1}'') = (38, 33)$ using the LSB matching revisited method. Since the original pixel x_i cannot be recovered by $y_i = \lfloor (x_i' + x_i'')/2 \rfloor = \lfloor (38 + 38)/2 \rfloor = 38$, the seven rules table is used for adjustment. Through Case-6, the final stego image pixels are $(x_i', x_{i+1}') = (x_i - 1, x_{i+1} + 2) = (36, 35)$ and $(x_i'', x_{i+1}'') =$

Table 1
The seven rules table.

Case	Pixel value differences				Final pixel values			
	$x_i - x_i'$	$x_{i+1} - x_{i+1}'$	$x_i - x_i''$	$x_{i+1} - x_{i+1}''$	x_i'	x_{i+1}'	x_i''	x_{i+1}''
1	0	0	−1	0	$x_i + 2$	$x_{i+1} + 1$	$x_i - 1$	$x_{i+1} + 1$
2	0	1	0	1	x_i	$x_{i+1} + 1$	x_i	$x_{i+1} - 1$
3	0	1	−1	0	$x_i + 2$	x_{i+1}	$x_i - 1$	x_{i+1}
4	−1	0	0	0	$x_i - 1$	x_{i+1}	$x_i + 2$	$x_{i+1} + 1$
5	−1	0	0	1	$x_i - 1$	x_{i+1}	$x_i + 2$	x_{i+1}
6	−1	0	−1	0	$x_i - 1$	$x_{i+1} + 2$	$x_i + 1$	$x_{i+1} - 1$
7	1	0	1	0	$x_i - 1$	$x_{i+1} - 1$	$x_i + 1$	$x_{i+1} + 2$

$(x_i + 1, x_{i+1} - 1) = (38, 32)$. After adjustment, the original image pixels can be recovered using $x_i = \lfloor (x_i' + x_i'')/2 \rfloor = \lfloor (36 + 38)/2 \rfloor = 37$ and $x_{i+1} = \lfloor (x_{i+1}' + x_{i+1}'')/2 \rfloor = \lfloor (35 + 32)/2 \rfloor = 33$.

$$\begin{cases} y_i = \lfloor (x_i' + x_i'')/2 \rfloor \\ y_{i+1} = \lfloor (x_{i+1}' + x_{i+1}'')/2 \rfloor \end{cases} \tag{2}$$

Besides, Sahu et al. [12] proposed the dual stego-imaging based reversible data hiding using improved LSB matching in 2019. In this paper, two reversible data hiding techniques are proposed, and the Technique 2 "Dual stego-image based modified LSB matching with reversibility" is related to our proposed method. The technique uses one cover image pixel x_i at a time. Two secret message bits (m_1, m_2) are embedded into the stego image pixels (x_i', x_i'') using Eqs. (3) (4) (5). Then distribute x_i' to stego image1, and x_i'' to stego image2.

$$(x_i', x_i'') = \begin{cases} (x_i, x_i + 1), & \text{if } (LSB(x_i) = m1) \text{ and } (AVG3(x_i) = m2) \\ (x_i, x_i), & \text{if } (LSB(x_i) = m1) \text{ and } (AVG3(x_i) \neq m2) \\ (x_i - 1, x_i + 1), & \text{if } (LSB(x_i) \neq m1) \text{ and } (AVG4(x_i) = m2) \\ (x_i + 1, x_i - 1), & \text{if } (LSB(x_i) \neq m1) \text{ and } (AVG4(x_i) \neq m2) \end{cases} \tag{3}$$

$$AVG3(x_i) = LSB(\left\lfloor \frac{x_i}{2} \right\rfloor + (x_i + 1)) \tag{4}$$

$$AVG4(x_i) = LSB(\left\lfloor \frac{x_i - 1}{2} \right\rfloor + (x_i + 1)) \tag{5}$$

2.3. The EMD related method

The EMD method is proposed by Zhang and Wang [17]. The embedding is performed n neighboring cover image pixels at a time, embed one secret digit in (2n+1)-ary notational system, where n is a system parameter ($n \geq 1$). Since each group has n pixels, there are 2n+1 possible ways of modification (include one case in which no pixel is changed). Based on this idea, at most, only one pixel is increased or decreased by 1. Therefore, the EMD method has good stego-image quality. To map these 2n+1 cases, the EMD method needs to define a one-to-one extraction function for the embedding and extraction procedure.

First, n neighboring pixels $(x_1, x_2, \ldots, x_n)$ are selected from the cover image. The extraction function is defined as $f(x_1, x_2, \ldots, x_n) = \left[\sum_{i=1}^{n} x_i \cdot i\right] \bmod (2n + 1)$. Suppose d is a secret digit in the (2n+1)-ary notational system. No modification is needed if d equals the value of the extraction function f When $d \neq f$ (), calculate $s = (d - f())$ mod (2n+1). If s is no more than n, increase the value of x_s by 1; otherwise, decrease the value of x_{2n+1-s} by 1.

In fact, the extraction function of EMD method can be represented as a 2D-matrix in Fig. 3. It calculates the value of all group pixels of (0, 0) to (255, 255) and generate 256 × 256 matrix to record this message for the embedding and extraction procedure. For example, if the cover image pixels are $(x_1, x_2) = (5, 3)$ and $d = 1$, then the stego image pixels are unchanged and $(x'_1, x'_2) = (5, 3)$. If $d = 2$, the stego image pixels will be $(x'_1, x'_2) = (6, 3)$. If $d = 3$, the stego image pixels will be $(x'_1, x'_2) = (5, 4)$. If $d = 4$, the stego image pixels will be $(x'_1, x'_2) = (5, 2)$. If $d = 0$, the stego image pixels will be $(x'_1, x'_2) = (4, 3)$.

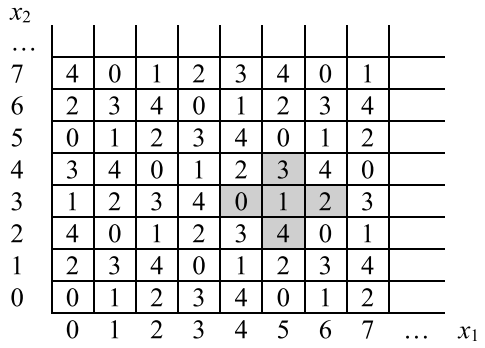

Fig. 3. 2D-matrix of EMD method ($n = 2$).

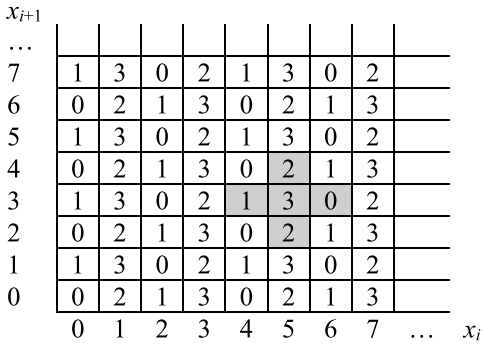

Fig. 4. 2D-matrix of LSB matching revisited method.

In 2015, Qin et al. [15] proposed a RDH scheme based on EMD with two stego images. In this scheme, the pixels in the first stego image are modified using the traditional EMD method, while the pixels in the second stego image are adaptively modified according to those in the first stego image in order to recover the original image. Thus the embedding procedure for the second stego image is more complicated and produce image quality loss. For the cover image Lena, the PSNR values for these two stego images are 52.11 dB and 41.34 dB, respectively. The hiding capacity is about 1.16 bpp. Besides, Lin et al. [16] proposed a dual-image-based reversible data hiding scheme with integrity verification using exploiting modification direction in 2019. This scheme embeds two 5-base secret digits into each pixel pair of the cover image simultaneously according to the EMD matrix to generate two stego pixel pairs. For the cover image Lena, the PSNR values for these two stego images are 52.39 dB and 49.24 dB, respectively. The hiding capacity is about 1.07 bpp. It can be seen that the image quality of these two stego images is unbalanced.

3. Proposed method

To improve Lu et al.'s method, a novel reversible dual images data hiding method based on the LSB matching revisited method and EMD is proposed. The new method provides the embedding capacity of about the same as Lu et al.'s, but with fewer changes to the cover image. This makes the stego images have better image quality and the original image can be recovered.

3.1. Transform LSB matching revisited to EMD

The LSB matching revisited method [3] is a modification to the LSB matching [2]. The embedding is performed for the two cover image pixels (x_i, x_{i+1}) at a time. After the embedding, two secret bits (m_1, m_2) are embedded and the stego image pixels are (x'_i, x'_{i+1}), where $m_1 =$

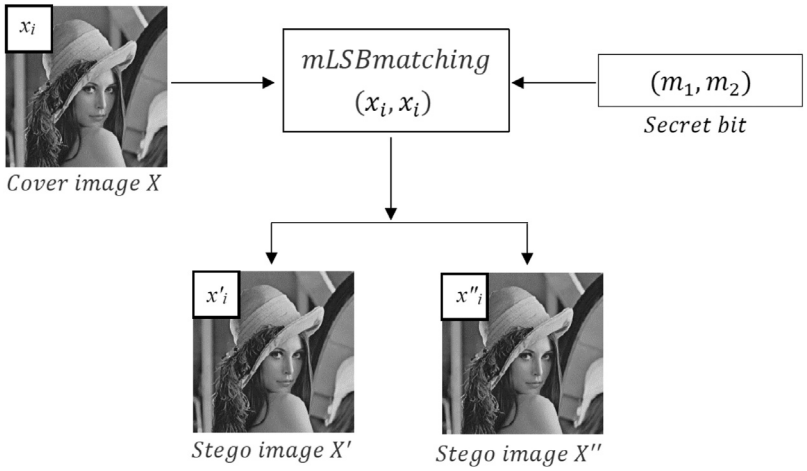

Fig. 5. The embedding flow diagram.

$\mathrm{LSB}(x'_i)$ and $m_2 = F\left(x'_i, x'_{i+1}\right) = \mathrm{LSB}(\lfloor x'_i/2 \rfloor + x'_{i+1})$. According to the embedding functions, we found that the LSB matching revisited method can be viewed as a kind of EMD method. The f_{EMD} extraction function for the LSB matching revisited method can be defined as:

$$f_{EMD}\left(x_i, x_{i+1}\right) = LSB\left(x_i\right) * 2 + LSB(\left\lfloor \frac{x_i}{2} \right\rfloor + x_{i+1}) \tag{6}$$

Fig. 4 shows the 2D-matrix using the f_{EMD} extraction function. Thus the embedding phase of LSB matching revisited method can be rewritten as follows:

Embedding Phase
Input: a pair of cover image pixels (x_i, x_{i+1}) two secret bits (m_1, m_2)
Output: a pair of stego image pixels (x'_i, x'_{i+1})

(1) Transform secret bits (m_1, m_2) to a decimal number s
(2) If $s == f_{EMD}\left(x_i, x_{i+1}\right)$:

$x'_i = x_i, x'_{i+1} = x_{i+1}$

else if s == $f_{EMD}\left(x_i - 1, x_{i+1}\right)$:

$x'_i = x_i - 1, x'_{i+1} = x_{i+1}$

else if s == $f_{EMD}\left(x_i + 1, x_{i+1}\right)$:

$x'_i = x_i + 1, x'_{i+1} = x_{i+1}$

else:

$x'_i = x_i, x'_{i+1} = x_{i+1} \pm 1$

For example, if the cover image pixels are $(x_i, x_{i+1}) = (5, 3)$ and the two secret bits are $(m_1, m_2) = (0, 1)$, then transform the secret bits to a decimal number $s = (01)_2 = 1$. $f_{EMD}(5,3) = LSB(5) * 2 + LSB\left(\left\lfloor \frac{5}{2} \right\rfloor + 3\right) = 3$. Since $s = f_{EMD}(4,3) = 1$, the stego image pixels are created $(x'_i, x'_{i+1}) = (4, 3)$. When extraction, $f_{EMD}(4,3) = 1$ is computed. Then transform it back to two binary bits $(01)_2$. The two secret bits are extracted correctly.

3.2. The proposed data embedding method

According to the 2D-matrix of LSB matching revisited method, the proposed data embedding method is designed as follows. The proposed method *mLSBmatching* does not use two cover image pixels at a time. Instead, it uses a single pixel. The single pixel is duplicated, embeds two secret bits, and then distributes to two stego images. The embedding flow diagram is shown in Fig. 5.

The *mLSBmatching* method is a modification of LSB matching revisited. It takes a single pixel value as input and duplicates the value. For example, if the single pixel value from the original cover image is 2, the pair (2, 2) is used in the *mLSBmatching* method. Fig. 6 shows the EMD extraction function f_{EMD} for the input pair (2, 2). If the secret message $s = 1$ and $f_{EMD}(2, 2) = 1$, then the stego pair (2, 2) will remain unchanged. If $s = 0$, then two pairs (2, 1) and (2, 3) can be the selected candidates. However, the pair (2, 1) is unable to recover the original pixel value 2 using the Eq. (8). Thus the pair (2, 3) is chose for the stego pair. If $s = 2$, then the pairs (1, 2), (3, 1) and (3, 3) can be the selected candidates. But only the stego pair (3, 1) can recover the original pixel using the Eq. (8). If $s = 3$, then the pairs (1, 1), (1, 3) and (3, 2) can be the selected candidates. Both the pair (1, 3) and (3, 2) can recover the original pixel using the Eq. (8), while the stego pair (3, 2) is chose with a shorter distance. Finally, the blocks with gray background are used for embedding.

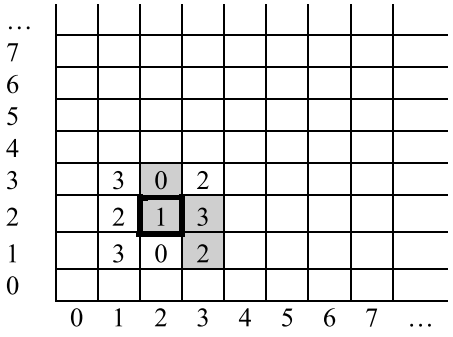

Fig. 6. The EMD extraction function f_{EMD} for pair (2, 2).

To summarize, the embedding phase of the proposed method *mLSBmatching* is shown as follows.

Embedding Phase of mLSBmatching using EMD function
Input: a pixel x_i from cover image two secret bits (m_1, m_2)
Output: a pair of stego image pixels (x'_i, x''_i)

(1) Transform secret bits (m_1, m_2) to a decimal number s
(2) if $s == f_{EMD}\left(x_i, x_i\right)$:

$x'_i = x_i, x''_i = x_i$

else if s == $f_{EMD}\left(x_i, x_i + 1\right)$:

$x'_i = x_i, x''_i = x_i + 1$

else if s == $f_{EMD}\left(x_i + 1, x_i - 1\right)$:

$x'_i = x_i + 1, x''_i = x_i - 1$

Fig. 7. 512 × 512 grayscale images for testing.

else if s == $f_{EMD}\left(x_i+1, x_i\right)$:

$x_i' = x_i + 1, x_i'' = x_i$

(3) Distribute x_i' to stego image1, and x_i'' to stego image2.

3.3. Data extraction and image recovery

The extraction phase of the proposed method is easy. For each pixel x_i' and x_i'' from two stego images, the secret message s is extracted using Eq. (7). Then the secret message s is transformed back to two binary bits (m_1, m_2). Finally the original pixel x_i can be recovered using Eq. (8).

$$s = f_{EMD}(x_i', x_i'') \tag{7}$$

$$x_i = \left\lfloor \frac{(x_i' + x_i'')}{2} \right\rfloor \tag{8}$$

In the same way, the secret message bits can be extracted using LSB matching revisited method, and the equations are shown in Eqs. (9) and (10).

$$m_1 = LSB\left(x_i'\right) \tag{9}$$

$$m_2 = LSB(\left\lfloor \frac{x_i'}{2} \right\rfloor + x_i'') \tag{10}$$

3.4. Underflow and overflow

To avoid the underflow and overflow problems, the pixels with values 0 or 255 are skipped for embedding. The pixels will remain unchanged. It means that if the original image pixel $x_i = 0$, then the stego pixel pair $(x_i', x_i'') = (0, 0)$. If $x_i = 255$, then the stego pixel pair $(x_i', x_i'') = (255, 255)$. When extraction, if the two stego image pixels are (0, 0) or (255, 255), then the extraction phase is skipped.

4. Experimental results

Fig. 7 shows the six 512 × 512 grayscale images, which are employed for testing, namely Lena, Mandrill, Pepper, Barbara, Boat and Zelda. The experiment uses peak signal noise ratio (PSNR) to measure the image quality. The higher the value of PSNR, the better the image quality is. The formula of PSNR is shown as follows:

$$PSNR = 10 \times \log\left(\frac{255^2}{\frac{1}{h \times w}\left(\sum_{i=1}^{h}\sum_{j=1}^{w}\left(X_{i,j}' - X_{i,j}\right)^2\right)}\right) \text{(dB)}, \tag{11}$$

Table 2
Results for the proposed method.

Images	PSNR1	PSNR2	SSIM1	SSIM2	Capacity	bpp
Lena	51.14	51.14	0.9980	0.9960	524,288	1.0000
Mandrill	51.14	51.14	0.9994	0.9987	524,210	0.9999
Pepper	51.14	51.14	0.9979	0.9962	524,240	0.9999
Barbara	51.14	51.14	0.9985	0.9970	524,288	1.0000
Boat	51.14	51.14	0.9981	0.9963	524,288	1.0000
Zelda	51.14	51.14	0.9978	0.9958	524,288	1.0000
Average	**51.14**	**51.14**	**0.9983**	**0.9967**	**524,267**	1.0000

where $h \times w$ is the image size, $x_{i,j}$ is the original pixel value, and $x'_{i,j}$ is the stego pixel value.

To measure the hiding capacity, the bits per pixel (bpp) is used. Since two stego images are used to carry the secret message bits, the total number of pixels is $2 \times h \times w$. The formula of bpp is shown as follows:

$$bpp = \frac{bits}{2 \times h \times w}, \tag{12}$$

where *bits* is the number of embedding bits.

Besides, the Structural Similarity Index SSIM [18] measures the similarity between the original image and the stego images. The formula of SSIM is shown as follows:

$$SSIM = \frac{(2\mu_x\mu_{x'} + C1)(2\sigma_{xx'} + C2)}{(\mu_x^2 + \mu_{x'}^2 + C1)(\sigma_x^2 + \sigma_{x'}^2 + C2)}, \tag{13}$$

where μ means mean pixel value and σ means the standard deviation, $\sigma_{xx'}$ is the covariance between the original image and stego image, $C1$ and $C2$ are constants.

Table 2 shows the image quality, image similarity and hiding capacity of the proposed method after embedding. The secret message is generated using MATLAB random number generator. The results are obtained from the average of 100 embedding test results. The PSNR1 and PSNR2 are the first and second stego image quality, respectively. The SSIM1 and SSIM2 are the first and second stego image similarity value, respectively. From the table, it can be seen that the stego image quality of our method is 51.14 dB. This improves the unbalanced stego image quality problem in the traditional EMD-based RDH. The SSIM value is close to 1 means the stego image and original image are highly similar. The hiding capacity is about 1 bpp.

Table 3 shows the results of Lu et al.'s method [7], and Table 4 shows the results of Sahu et al.'s Technique 2: Dual stego-image based modified LSB matching with reversibility [12]. Table 5 show the comparison of these three methods. From the table, it can be seen that the stego image quality (PSNR2) of our method is better than that of Lu

Table 3
Results for Lu et al.'s method.

Images	PSNR1	PSNR2	SSIM1	SSIM2	Capacity	bpp
Lena	49.13	49.12	0.9942	0.9958	524,288	1.0000
Mandrill	47.95	49.15	0.9985	0.9983	522,996	0.9975
Pepper	49.11	49.08	0.9953	0.9950	524,192	0.9999
Barbara	49.14	49.11	0.9971	0.9965	524,208	0.9998
Boat	49.00	49.07	0.9966	0.9963	524,208	0.9998
Zelda	49.14	49.09	0.9949	0.9945	524,288	1.0000
Average	**48.91**	**49.10**	**0.9961**	**0.9960**	**524,030**	**0.9995**

Table 4
Results for Sahu et al.'s method.

Images	PSNR1	PSNR2	SSIM1	SSIM2	Capacity	bpp
Lena	51.17	49.41	0.9960	0.9945	524,288	1.0000
Mandrill	51.16	49.41	0.9987	0.9982	524,288	1.0000
Bridge	51.21	49.50	0.9986	0.9980	524,288	1.0000
Couple	51.18	49.42	0.9974	0.9964	524,288	1.0000
Boat	51.18	49.41	0.9971	0.9992	524,288	1.0000
House	51.18	49.42	0.9972	0.9962	524,288	1.0000
Average	**51.18**	**49.43**	**0.9975**	**0.9970**	**524,288**	**1.0000**

Table 5
Comparison results with Lu and Sahu.

	PSNR1	PSNR2	SSIM1	SSIM2	Capacity	bpp
Proposed method	51.14	51.14	0.9983	0.9967	524,267	1.0000
Lu et al. [7]	48.91	49.10	0.9958	0.9963	524,030	0.9995
Sahu et al. [12]	51.18	49.43	0.9975	0.9970	524,288	1.0000

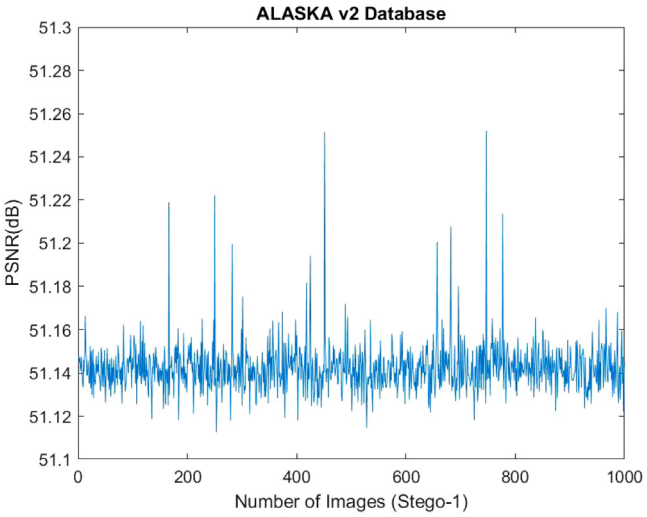

Fig. 8. PSNRs of stego image 1 using ALASKA.

et al.'s and Sahu et al.'s. As to the hiding capacity and image similarity, the performance result is superior to Lu and is similar with Sahu.

A large image dataset ALASKA#2 (https://alaska.utt.fr/) is also used for performance evaluation. This dataset is made of a set of 80,000 raw images. The first 1000 images (image no. 00001~01000) are employed for testing in our experiment. Figs. 8 and 9 show the stego image quality (PSNR), and the hiding capacity is in Fig. 10. The average PSNR of stego images 1 is 51.1425, the average PSNR of stego images 2 is 51.1423, and the average bpp is 0.9997. The results of large database performance evaluation coincide with Table 5.

Steganography involves hiding information in cover images to obtain the stego images, in such a way that the cover image is perceived not to have any embedded message for its unintended recipients. In contrast to steganography, steganalysis [2,19–22] is focused on detecting the presence of hidden messages in cover images. Oswaldo

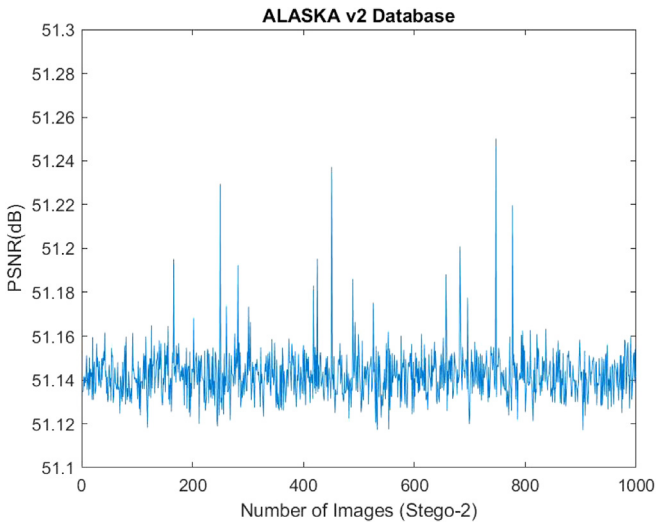

Fig. 9. PSNRs of stego image 2 using ALASKA.

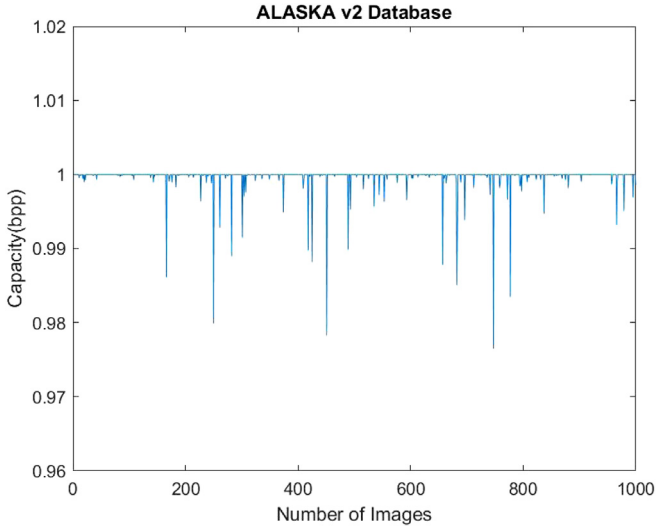

Fig. 10. Hiding capacity (bpp) using ALASKA.

et al. [19] proposed an image-adaptive steganalysis for LSB Matching steganography in 2016. The method extracts content features in the image for and analyzes the statistical noise. The most well-known steganalysis for LSB embedding is RS (Regular and Singular) detection [22]. In order to prove that the proposed method is secure, the RS detection is applied to the proposed method.

RS detection flips the LSBs and divides the pixels into three groups: R(Regular Group), S(Singular Group), U(Unusable Group). Then a statistical method is used to determine whether the images carry information or not. In a typical image, the expected value of R_M equals that of R_{-M}, and the same is true for S_M and S_{-M}. Fig. 11 shows the RS-analysis results for the proposed method. The $R_M \approx R_{-M}$ and $S_M \approx S_{-M}$ on each test images. The results reveal that the proposed method is secure.

5. Conclusions

In the paper, we found that the LSB matching revisited method can be viewed as a kind of EMD method. According to this finding, a simple modified LSB matching method using the dual images is proposed based on the 2D EMD matrix. The proposed method improves the quality of

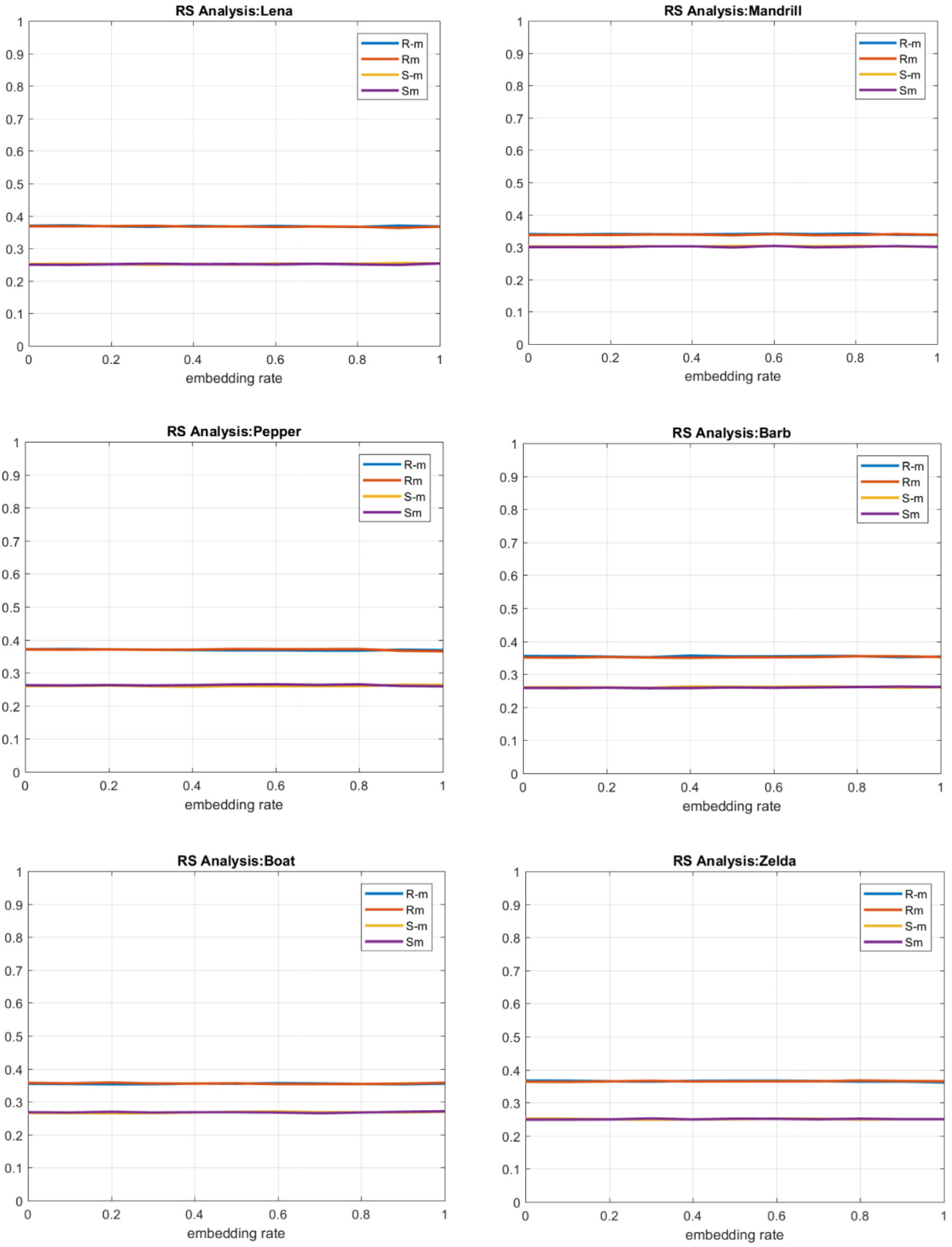

Fig. 11. RS-analysis of test images in the proposed method.

stego images and provides the same hiding capacity compared with previous works. Additionally, the modified LSB matching method also guarantees that the original image can be recovered from the dual stego images. The proposed method also improves the unbalanced stego image quality problem in the traditional EMD-based RDH. Experimental results show that the image qualities of dual stego images are both 51.14 dB. The SSIM value is close to 1 means the stego image and original image are highly similar. The hiding capacity is about 1 bpp. Besides, the proposed method is secure against RS-analysis.

CRediT authorship contribution statement

Hsien-Wen Tseng: Conceptualization, Methodology, Writing – review & editing. **Hui-Shih Leng:** Software, Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The study is supported by Ministry of Science and Technology (MOST) Taiwan, R.O.C. under MOST 109-2221-E-324-020.

References

[1] L.F. Turner, Digital data security system, 1989, Patent IPN WO 89/08915.
[2] A. Ker, Improved detection of LSB steganography in grayscale images, in: Proc. Information Hiding Workshop, in: Springer LNCS, vol. 3200, 2004, pp. 97–115.
[3] J. Mielikainen, LSB matching revisited, in: IEEE Signal Processing Letters, 2006, pp. 285–287.
[4] H. Hiary, K.E. Sabri, M.S. Mohammed, A hybrid steganography system based on LSB matching and replacement, Int. J. Adv. Comput. Sci. Appl. 7 (9) (2016) 374–380.
[5] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forensics Secur. 5 (2) (2010) 201–214.
[6] Y.L. Wang, J.J. Shen, M.S. Hwang, An improved dual image-based reversible hiding technique using LSB matching, Int. J. Netw. Secur. 19 (5) (2017) 858–862.
[7] T.C. Lu, C.Y. Tseng, J.H. Wu, Dual imaging-based reversible hiding technique using LSB matching, Signal Process. 108 (2015) 77–89.
[8] T.C. Lu, J.H. Wu, C.C. Huang, Dual-image-based reversible data hiding method using center folding strategy, Signal Process. 115 (2015) 195–213.
[9] C.F. Lee, Y.L. Huang, Reversible data hiding scheme based on dual stegano-images using orientation combinations, Telecommun. Syst. 52 (4) (2013) 2237–2247.
[10] T.C. Lu, L.P. Chi, C.H. Wu, Reversible data hiding in dual stego-images using frequency-based encoding strategy, Multimedia Tools Appl. 76 (22) (2017) 23903–23929.
[11] H.W. Tseng, H.X. Lu, H.S. Leng, Dual image reversible data hiding based on modified LSB matching method, in: 2018 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Sendai, Japan, 2018.
[12] A.K. Sahu, G. Swain, Dual stego-imaging based reversible data hiding using improved LSB matching, Int. J. Intell. Eng. Syst. 12 (5) (2019) 63–73.
[13] A.K. Sahu, G. Swain, High fidelity based reversible data hiding using modified LSB matching and pixel difference, J. King Saud Univ. - Comput. Inf. Sci. (2019) http://dx.doi.org/10.1016/j.jksuci.2019.07.004.
[14] A.K. Sahu, G. Swain, Reversible image steganography using dual-layer LSB matching, Sens. Imaging 21 (1) (2020) 1–21.
[15] C. Qin, C.C. Chang, T.J. Hsu, Reversible data hiding scheme based on exploiting modification direction with two steganographic images, Multimedia Tools Appl. 74 (2015) 5861–5872.
[16] J.Y. Lin, Y. Chen, C.C. Chang, Y.C. Hu, Dual-image-based reversible data hiding scheme with integrity verification using exploiting modification direction, Multimedia Tools Appl. 78 (2019) 25855–25872.
[17] X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Commun. Lett. 10 (11) (2006) 781–783.
[18] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: From error visibility to structural similarity, IEEE Trans. Image Process. 13 (4) (2004) 600–612.
[19] J.S. Oswaldo, C.H. Manuel, N.M. Mariko, P.M. Hector, T.M. Karina, Image-adaptive steganalysis for LSB matching steganography, in: 2016 39th International Conference on Telecommunications and Signal Processing (TSP), Vienna, 2016, pp. 478–483.
[20] X. Chen, G. Gao, D. Liu, Z. Xia, Steganalysis of LSB matching using characteristic function moment of pixel differences, in: China Communications, IEEE, 2016, pp. 66–73.
[21] G. Yang, X. Li, B. Li, Z. Guo, A new detector of LSB matching steganography based on likelihood ratio test for multivariate Gaussian covers, in: 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), IEEE, Hong Kong, China, 2015, pp. 757–760.
[22] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia 8 (4) (2001) 22–28.