A Hybrid Steganography System based on LSB Matching and Replacement

Hazem Hiary and Khair Eddin Sabri
Computer Science Department,
The University of Jordan, Amman, Jordan

Mohammed S. Mohammed and Ahlam Al-Dhamari
Computer Engineering Department,
Hodeidah University, Hodeidah, Yemen

Abstract—**This paper proposes a hybrid steganographic approach using the least significant bit (LSB) technique for grayscale images. The proposed approach uses both LSB matching (LSB-M) and LSB replacement to hide the secret data in images. Using hybrid LSB techniques increase the level of security. Thus, attackers cannot easily, if not impossible, extract the secret data. The proposed approach stores two bits in a pixel. The embedding rate can reach up to 1.6 bit per pixel. The proposed approach is evaluated and subjected to various kinds of image processing attacks. The performance of the proposed algorithm is compared with two other relevant techniques; pixel-value differencing (PVD) and Complexity Based LSB-M (CBL). Experimental results indicate that the proposed algorithm outperforms PVD in terms of imperceptibility. Also, it significantly outperforms CBL in two main features; higher embedding rate (ER), and more robust to most common image processing attacks such as median filtering, histogram equalization, and rotation.**

Keywords—*Steganography; LSB matching; LSB replacement; Embedding capacity; Imperceptibility*

I. INTRODUCTION

These days data transmission on the digital communications via the internet confronts a wide range of security issues [1], [2], [3]. Consequently, powerful digital techniques are needed to protect data during its transmission on the internet. One of the great interest solutions used to protect data is steganography [4], [5], [6]. Steganography is the art of invisible communication by hiding a secret message in a digital cover media such as images [7], [8], text [9], audio [10], video [11] and network traffic [12], without being dubious [13], [14]. Because digital images have a great deal of redundant data, there has been an increased interest in utilizing them as cover media for steganographic purposes [15], [16].

Image steganographic algorithms can be classified in terms of the embedding domain into two main classes: spatial domain and frequency domain-based algorithms [17], [18]. Spatial domain-based algorithms conceal secret message straightforwardly in the intensity of pixels of an image, while in frequency domain-based algorithms, the image is firstly transformed into its frequency domain and secret message is then concealed in the transform coefficients [19], [20].

LSB replacement is one of the most well-known methods in the spatial domain [21]. In this method, a secret data is embedded into a cover image by replacing the LSBs of the cover image pixels with secret data bits to get the stego image [22], [23]. For a cover image, LSB replacement increases the even pixels by one or abandons them unaltered, while it decreases

the odd pixels by one or leaves them unchanged [24]. Due to the feeble sensibility of the human visual system (HVS), the presence of the embedded secret data cannot be perceptible. The quality of the stego image presented by LSB replacement may not be tolerable if a large amount of LSB is to be used in the embedding process. As a case, a stego image can accomplish as low as 31.78 dB of the PSNR by utilizing LSB-4 replacement [25]. Numerous credible steganographic methods have been devised for LSB replacement method [26].

LSB matching (LSB-M) method was proposed in [27], which is also called ±1 embedding [28]. In this scheme, the pixel value of the cover image is increased or decreased randomly by one when the secret bit is not equal to the LSB of the cover image pixel [5]. The LSB-M changes both the histogram of an image and the correlation between adjacent pixels and this helps steganalysis methods to attack this method [29].

In [18], the authors proposed a method called Complexity Based LSB-M (CBL). The method employs the strategy of adaptivity and the use of LSB-M in order to increase the security against attacks. CBL uses a local neighborhood analysis for determination of secure locations of an image and then it uses LSB-M for the embedding purpose.

In this paper, a hybrid approach using both LSB-M and LSB replacement methods is proposed. The approach is an improvement over the CBL method in order to increase both the embedding capacity and the robustness. The proposed approach stores two bits of the secret bits in a pixel. One bit is stored in the seventh bit using LSB-M technique; the other bit is stored in the eighth bit using LSB replacement technique. Thus, the maximum embedding capacity is increased to double (1.6) bits per pixel (bpp) compared to CBL maximum embedding capacity (0.8). This approach does not produce any distortions to be suspected by unauthorized observers and yields lower computational costs in its embedding and extraction processes. Moreover, it provides more robustness against most image processing attacks.

The remainder of this paper is organized as follows: In Section II a number of LSB-M based algorithms are represented. In Section III the embedding and extracting procedures for the proposed algorithm are presented. Experimental results and comparisons between the algorithm and other related algorithms are presented in Section IV. Finally, conclusions and future directions are given in Section V.

II. RELATED WORKS

The literature is worth of the contributions in the field of LSB steganography. The work in [30] proposed pixel-value differencing (PVD) method. The main idea behind PVD is to use the difference of two consecutive pixels of a grayscale image to hide data. In their method, a pixel-value differencing is used to distinguish between edge areas and smooth areas. Consequently, the capacity of embedded data in edge areas is higher than that of smooth areas. Recently, to enlarge the embedding efficiency on PVD method, a lot of methods were proposed by combining PVD and LSB replacement methods, such as [31], [32], [33]. With a slight alteration to the original PVD technique, the side match technique which is based on the correlation of a pixel with its neighboring pixels has additionally been evolved. In [34], the authors presented 2, 3 and 4-sided side match methods by using the correlation of a target pixel with its 2, 3, and 4 neighboring pixels.

Dissimilar to LSB replacement and LSB-M, LSB matching revisited (LSB-MR) uses a pair of pixels as hidden unit instead of one pixel [21]. This method uses grayscale cover images. The embedding process is performed on a cover pixel pair (g_i, g_{i+1}) at a time to embed a secret bit pair (b_i, b_{i+1}). The corresponding stego pixel pair (g'_i, g'_{i+1}) can be obtained by keeping g_i and g_{i+1} unaltered, or by increasing or decreasing them by one. The method used the function $y = f(g_i, g_{i+1}) = LSB(\lfloor g_i/2 \rfloor + g_{i+1})$ to evaluate whether or not the pixel values g_i and g_{i+1} need alteration. However, on average, the embedding rate (bpp) for both LSB-M and LSB-MR is about 1 bpp, which is poor. A generalized LSB-M scheme (G-LSB-M) was proposed in [35] to generalize the method in [21]. To enhance the level of security of both LSB-M and G-LSB-M, a content adaptive method was proposed in [36]. In this method, if the secret bit does not match the LSB of corresponding cover image pixel, the decision of alteration direction is not arbitrary and is attempted to have the best correlation with the neighboring pixels. In [37], an approach called (ALSBMR) used LSB-MR with adaptive embedding.

In [18], the authors proposed LSB-M adaptive steganography algorithm called Complexity Based LSB-M (CBL). They used an 8-neighborhood of a pixel to determine the complexity region for embedding data in that region. They used LSB-M to embed data. The drawback of CBL algorithm is the low embedding capacity where it can not embed more than one bit in a pixel. This drawback is overcome in the proposed work by using LSB-M and LSB replacement techniques to increase the embedding capacity.

In [38], the authors proposed a data hiding algorithm based on interpolation, LSB substitution, and histogram shifting. In this work interpolation is used to adjust embedding capacity with low image distortion, the embedding process is then applied using LSB substitution and histogram shifting methods. In [39], the LSB substitution is improved by using a bit inversion technique. In this work secret data is hidden after compressing smooth areas of the image losslessly, resulting in fewer number of modified cover image pixels. A bit inversion technique is then applied where certain LSBs of pixels are modified if they occur in a particular pattern. In [40], a semi-reversible data hiding method which employs interpolation and LSB substitution is proposed. Interpolation is first used to scale up and down the cover image before hiding secret data to

achieve high embedding capacity with low image distortion. Then, embedding is done using the LSB substitution method.

III. PROPOSED ALGORITHM

Embedding capacity, visual quality of stego image (imperceptibility), efficiency regarding execution time and the security level (robustness) are four primary criteria that are utilized to evaluate the performance of the steganographic scheme. The proposed algorithm uses both LSB-M and LSB replacement to address these criteria. An adaptive algorithm that is a modification to CBL approach [18] is proposed. Details of embedding and extraction phases are presented in the next lines.

A. Embedding phase

In the embedding phase, the algorithm embeds two bits in the pixels that have complexity value equal or more than a threshold value. One bit is embedded using LSB-M in the seventh bit from the left; another bit is embedded using LSB replacement in the least significant bit. The embedding phase is illustrated in the diagram shown in Fig. 1.
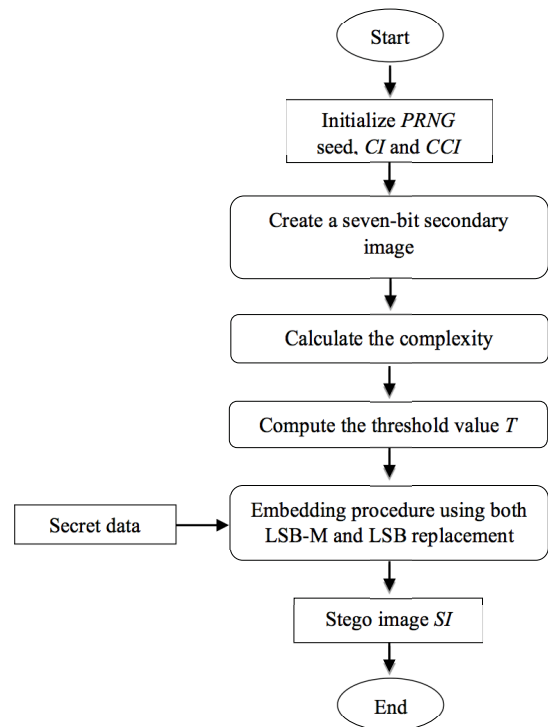

Fig. 1. Flow diagram of the embedding phase

The proposed embedding algorithm is based on CBL algorithm [18]. Step 2 and step 5 in CBL algorithm were modified to achieve more capacity. In step 2, the least significant bit is removed and only the first seven bits are used to create the secondary image. In step 5, both LSB-M and LSB replacement are used to embed two bits of the secret data in the selected pixels. The proposed embedding algorithm is described in the following steps.

Step 1. Initialization: In this step, number of variables are initialized as follows:

Set $PRNG$ seed
CI $\leftarrow$ cover image
CCI $\leftarrow$ copy of cover image
$[M, N]$ $\leftarrow$ dimensions of cover image

where $PRNG$ is a pseudo random number generator, $PRNG$ is initialized by a seed, which is a number that have to be selected and shared between the sender and the receiver.

Step 2. Secondary image formation: In this step, the least significant bit of each pixel in CI is removed and only the first seven bits are used to create the secondary image. This image will be used to compute the complexity values of pixels in the next step. Using the secondary image helps the receiver to get the same complexity value [18]. The following routine creates this image.

> **for** each pixel $CI(x, y)$ **do**
> $r \leftarrow$ random number $\in [0, 1]$
> $CI(x, y) = bitshift(CI(x, y), -1)$
>   **if** $CI(x, y)$ is odd **then**
>   **if** $r \leq 0.5$ **then**
> $CI(x, y) \leftarrow CI(x, y) + 1$
>   **else**
> $CI(x, y) \leftarrow CI(x, y) - 1$
>   **end if**
>   **end if**
> **end for**

where $bitshift$ function will shift the pixel bits to the right, so it will remove the least significant bit. For example, if the pixel value is $(215)_{10} = (11010111)_2$, then the pixel value after the shifting process will be $(1101011)_2 = (107)_{10}$.

Step 3. Pixel complexity computation: The complexity of each pixel is computed by adding absolute values of differences of the pixel with its neighbors as follows [18]

$$Complexity(x, y) = \sum_{i=-1}^{1} \sum_{j=-1}^{1} |CI(x, y) - CI(x+i, y+j)| \tag{1}$$

Figure 2 shows the neighborhood of pixel $CI(x, y)$. The complexity value is an indication of the type of region that the pixel belongs to; edge or smooth region. Where more data can be embedded in edge regions without creating any suspicion. A high complexity value indicates the pixel is located in an edge region, while a low value indicates the pixel is located in a smooth region. Examples of cover images and their complexity values are illustrated in Fig. 3.

$CI(x-1, y-1)$	$CI(x-1, y)$	$CI(x-1, y+1)$
$CI(x, y-1)$	$CI(x, y)$	$CI(x, y+1)$
$CI(x+1, y-1)$	$CI(x+1, y)$	$CI(x+1, y+1)$

Fig. 2. 8-neighbors of pixel $CI(x, y)$

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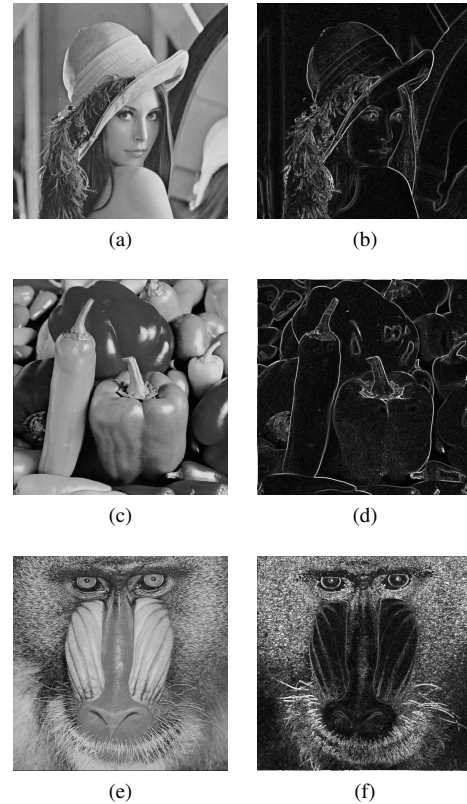
(c)   (d)

(e)   (f)

Fig. 3. Cover images (left) and their octonary-complexity values (right)

Step 4. Threshold computation: Complexity values of pixels are compared with a threshold; values greater than or equal to threshold indicate an edge region, and smooth region otherwise. To calculate threshold value, the number of pixels to be embedded (NP) must be computed using $NP = SB/2$, where SB refers to the total number of embedded secret bits. The threshold value T is chosen to make sure that at least NP of the pixels are complex. The following routine shows how T is computed.

> $t_{\circ} \leftarrow 127$
> $n \leftarrow 0$
> L:
> **for** each pixel $Complexity(x, y)$ **do**
>   **if** $t_{\circ} \geq Complexity(x, y)$ **then**
> $n \leftarrow n + 1$
>   **end if**
> **end for**
> **if** $n < NP$ AND $t_{\circ} \neq 0$ **then**
> $t_{\circ} = t_{\circ} - 1$
>   go to L
> **else**
> $T = t_{\circ}$
> **end if**

where $t_{\circ}$ is a temporary value of threshold, which starts with the maximum value of the seven-bit pixel.

Step 5. Embedding: In this step, the secret data are embedded using LSB-M and LSB replacement techniques. Two bits are embedded in each selected pixel; the first one is embedded using LSB-M as in CBL but in the seventh bit, the second bit

is embedded in the least significant bit using LSB replacement.

The following pseudocode presents the embedding procedure, where s is the string of message bits and SI is the stego image.

The last four lines of the algorithm present the proposed modification on this step. The selected pixel value of the secondary image is converted to seven bits binary by using $dec2bin$ function and stored in $conca$. One of the secret bits is concatenated to the seven bits in $conca$ by using $strcat$ function and stored in emb. Finally, the eight bits in emb are converted to decimal value by using $bin2dec$ function and the resulting value is stored in SI.

```
set PRNG
n ← 0
for each pixel CI(x, y) do
    r ← random number ∈ [0, 1]
    if CI(x, y) = 0 OR Complexity(x, y) < T then
        SI(x, y) ← CCI(x, y)
    else
        if CI(x, y) mod 2 ≠ s(n) then
            if r ≤ 0.5 then
                SI(x, y) ← CI(x, y) − 1
            else
                SI(x, y) ← CI(x, y) + 1
            end if
        end if
        n ← n + 1
        conca ← dec2bin(SI(x, y), 7)
        emb ← strcat(conca, s(n))
        SI(x, y) ← bin2dec(emb)
        n ← n + 1
    end if
end for
```

B. Extraction phase

The extraction phase is the same as embedding in the first four steps, except that the stego image SI is used instead of the cover image to create the secondary image and compute the complexity, and a copy of stego image CSI is created to be used in the extraction step. Figure 4 shows the flow diagram of the extracting phase.

After the first four steps are done, the extraction step works by extracting the two least significant bits of each pixel that is labeled as complex. The following pseudocode presents the extraction routine, where mod 4 is used to extract the two least significant bits as a decimal number, the $dec2bin$ function is used to convert the decimal number back to two binary bits, which are stored in s.

```
n ← 0
for each pixel SI(x, y) do
    if SI(x, y) ≠ 0 AND Complexity(x, y) ≥ T then
        sec ← CSI(x, y) mod 4
        s(n : n + 1) ← dec2bin(sec)
        n ← n + 2
    end if
end for
```
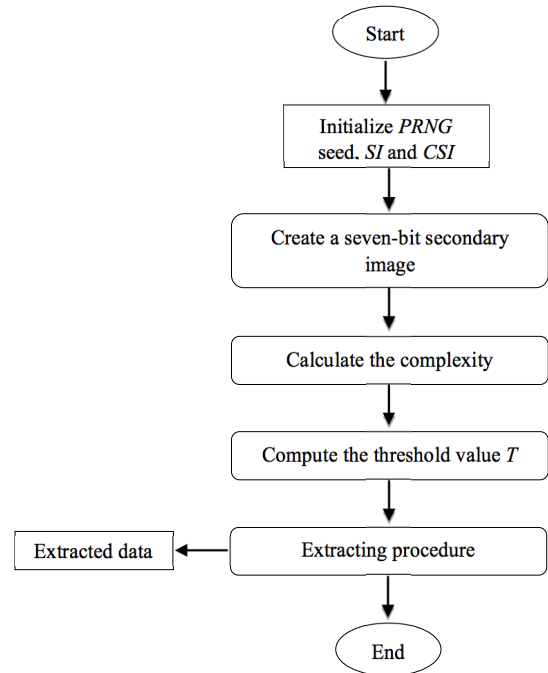

Fig. 4. Flow diagram of the extraction phase

IV. EXPERIMENTAL RESULTS AND COMPARISONS

Here, experimental results are presented to demonstrate the performance of the proposed algorithm. Several grayscale test images of size 512×512 were used from [41], [42]. Sample of these images is shown in Fig. 5.

Generally, the steganographic algorithms can be evaluated by two benchmarks; the embedding rate and the imperceptibility (or the quality of the stego image). The embedding rate (ER) is defined as the number of secret data bits that can be embedded per pixel, it can be calculated as [43], [44]

$$ER = \frac{SB}{M \times N} \quad (bpp) \tag{2}$$

where SB refers to the total number of embedded secret bits, M and N are the width and height of the cover image, respectively. To gauge the imperceptibility or the quality of the stego image, the peak signal-to-noise ratio (PSNR) is used. A high PSNR value indicates a high similarity between the stego and cover images, while a low value demonstrates the opposite. PSNR can be computed as [30], [45]

$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \quad (dB) \tag{3}$$

where MAX is the maximum value of the pixel intensity, e.g., $MAX = 255$ for 8-bit grayscale images. MSE is the mean square error, defined as

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (CI(i, j) - SI(i, j))^2 \tag{4}$$

Figure 6 shows stego images for five cover images using the proposed algorithm. The PSNR values range between 47.77dB and 48.13dB when the embedding rate is 0.8 bpp, and between

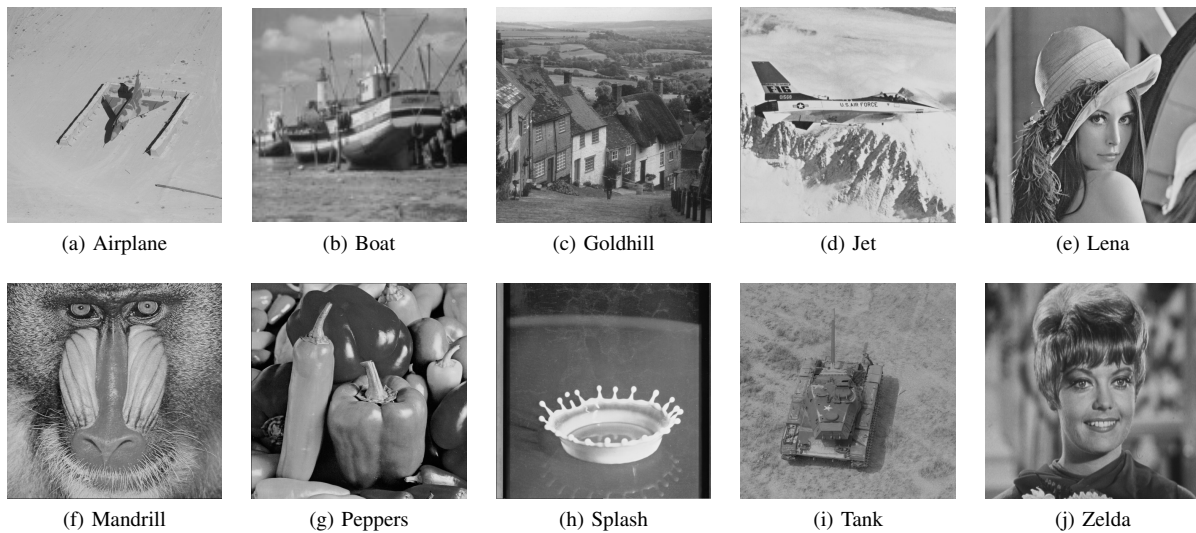| (a) Airplane | (b) Boat | (c) Goldhill | (d) Jet | (e) Lena |
| (f) Mandrill | (g) Peppers | (h) Splash | (i) Tank | (j) Zelda |

Fig. 5. Sample test images used in the experiments

44.93dB and 45.09dB when the embedding rate is 1.6 bpp. However, in all cases, there is no distortion to be aware of by the human eye.

To evaluate the proposed approach, a comparison was conducted with other approaches: PVD [30] and CBL [18]. Table I presents this comparison, where four embedding rates (0.3, 0.5, 0.8 and 1.6 bpp) were used for each method, and the PSNR average is calculated for the 10 test images.

TABLE I. IMPERCEPTIBILITY AND ER COMPARISON BETWEEN THE PROPOSED APPROACH AGAINST PVD [30] AND CBL [18]

Approach	ER (bpp)	PSNR average (dB)
PVD	0.3	49.72
	0.5	47.30
	0.8	44.81
	1.6	41.83
CBL	0.3	56.16
	0.5	53.95
	0.8	51.94
	1.6	–
Proposed	0.3	52.24
	0.5	50.00
	0.8	47.97
	1.6	45.06

Since CBL cannot embed 1.6 bpp, the corresponding PSNR value is left as (–). It is noticeable that the proposed algorithm in all test images and embedding rates provides better imperceptibility values than PVD. Moreover, compared to CBL, the approach provides double embedding rate. However, average PSNR values are less; this is because CBL only embeds one bit per pixel, while the approach embeds two bits.

To further evaluate the proposed approach, the stego images were subjected to different kinds of image processing attacks, namely JPEG 2000 lossy, sharpening, Gaussian noise, median filter, contrast enhancement, Gaussian filter, histogram equalization, and rotation. Table II shows the average bit correct rate (BCR) [46] of the watermarks after applying these attacks at embedding rate 0.8 bpp. It is worth mentioning that the BCR

can be computed using

$$BCR = \frac{L - \sum_{i=1}^{L} OB \oplus EB}{L} \qquad (5)$$

where OB is the original bit and EB is the extracted bit of the watermark. L is the length of the watermark.

The obtained results show that the proposed algorithm is more robust than CBL against median filtering, histogram equalization and rotation attacks. BCR values after applying JPEG 2000 lossy, sharpening, Gaussian noise and contrast enhancement were similar. All BCR values are low (between 0.48 and 0.63) because the attacks change the secondary image of stego image.

TABLE II. AVERAGE BCR COMPARISON AFTER IMAGE ATTACKS BETWEEN THE PROPOSED APPROACH AND CBL [18]

Attack	CBL	Proposed
JPEG 2000 lossy	0.50	0.50
Sharpening 3×3	0.50	0.50
Gaussian noise (0,0.001)	0.50	0.50
Median filter 3×3	0.52	0.63
Contrast Enhancement	0.50	0.50
Gaussian filter 3×3	0.50	0.48
Histogram equalization	0.50	0.54
Rotation $35°$	0.53	0.58
Rotation $75°$ **w/auto-crop**	0.53	0.58

V. CONCLUSIONS AND FUTURE WORK

In this paper, by considering the significance of the embedding efficiency of steganographic algorithms, a hybrid approach is proposed for data hiding with high capacity and robustness. The proposed approach is a modification to CBL to achieve more embedding capacity. The proposed approach uses both LSB-M and LSB replacement techniques to conceal secret data in the least significant two bits of the pixel values. Thus, the proposed approach can achieve more embedding capacity than CBL, which only embeds secret data in the least significant bit of pixel values.

The maximum embedding rate achieved by the proposed approach is 1.6 bpp, which is double of the capacity achieved

(a) Lena   (b) PSNR=47.93   (c) PSNR=44.98

(d) Peppers   (e) PSNR=47.94   (f) PSNR=45.06

(g) Mandrill   (h) PSNR=48.13   (i) PSNR=45.09

(j) Splash   (k) PSNR=47.77   (l) PSNR=44.93

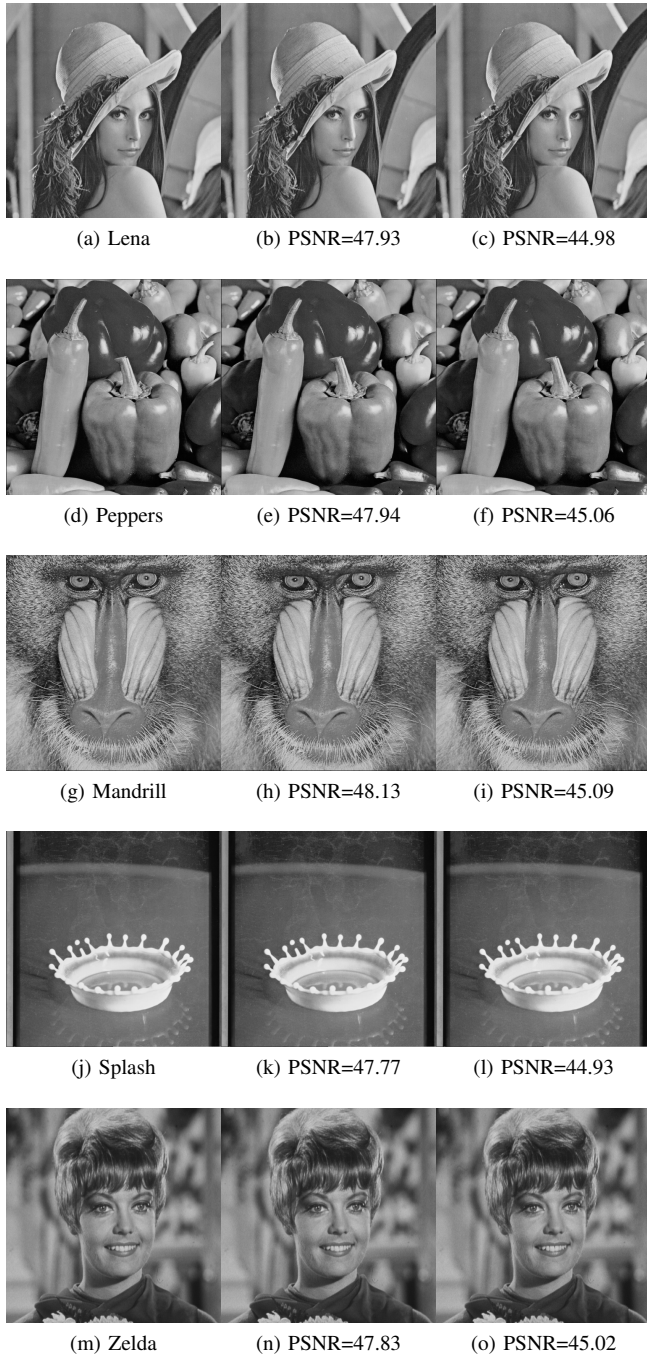(m) Zelda   (n) PSNR=47.83   (o) PSNR=45.02

Fig. 6. Cover images (left), stego images with ER=0.8 bpp (middle), and ER=1.6 bpp (right)

by CBL. By comparing the proposed approach to PVD and CBL, the imperceptibility over PVD is improved, embedding capacity is also improved over CBL, without distorting the stego images. The watermarks in the approach are more robust than CBL when subjected to some common attacks.

Since the approach is based on CBL algorithm, future plans include proposing a new algorithm that achieves a higher embedding rate than what is accomplished (1.6 bpp), and improve the imperceptibility.

REFERENCES

[1] N. Hamid, A. Yahya, R. Ahmad, and O. Al-Qershi, "Image steganography techniques: an overview", International Journal of Computer Science and Security (IJCSS), vol. 6, no. 3,pp. 168–187, 2012.

[2] C. Gayathri and V. Kalpana, "Study on image steganography techniques", International Journal of Engineering and Technology (IJET), vol. 5, no. 2, pp. 572–577, 2013.

[3] L. Saini and V. Shrivastava, "A survey of digital watermarking techniques and its applications", International Journal of Computer Science Trends and Technology (IJCST), vol. 2, no. 3, pp. 70–73, 2014.

[4] A. Tiwari, S. Yadav, and N. Mittal, "A review on different image steganography techniques", International Journal of Engineering and Innovative Technology (IJEIT), vol. 3, no. 7, pp. 121–124, 2014.

[5] F. Huang, Y. Zhong, and J. Huang, "Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm", Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 8389, pp. 19–31, 2014.

[6] M. Khosravi and A. Naghsh-Nilchi, "A novel joint secret image sharing and robust steganography method using wavelet", Multimedia systems, vol. 20, no. 2, pp. 215–226, 2014.

[7] B. Mohd, S. Abed, B. Na'ami, and T. Hayajneh, "Hierarchical steganography using novel optimum quantization technique", Signal, Image and Video Processing (SIViP), vol. 7, no. 6, pp. 1029–1040, 2013.

[8] X. Li, W. Zhang, B. Ou, and B. Yang, "A brief review on reversible data hiding: current techniques and future prospects". Proc. IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP), Xi'an, China, 2014, pp. 426–430.

[9] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in text by using MS word symbols". Proc. Zone 1 Conference of the American Society for Engineering Education (ASEE Zone 1), Bridgeport, CT, USA, 2014, pp. 1–5.

[10] P. Pathak, A. Chattopadhyay, and A. Nag, "A new audio steganography scheme based on location selection with enhanced security". Proc. International Conference on Automation, Control, Energy and Systems (ACES), Hooghy, India, 2014, pp. 1–4.

[11] M. Beno, A. George, I. Valarmathi, and S. Swamy, "Hybrid optimization model of video steganography technique with the aid of biorthogonal wavelet transform", Journal of Theoretical and Applied Information Technology, vol. 63, no. 1, pp. 190–199, 2014.

[12] W. Mazurczyk, P. Szaga, and K. Szczypiorski, "Using transcoding for hidden communication in IP telephony", Multimedia Tools and Applications, vol. 70, no. 3, pp. 2139–2165, 2014.

[13] N. Johnson, Z. Duric, and S. Jajodia, "Information hiding: steganography and watermarking–attacks and countermeasures", Kluwer, USA, 2001.

[14] G. Liu, W. Liu, Y. Dai, and S. Lian "Adaptive steganography based on block complexity and matrix embedding", Multimedia systems, vol. 20, no. 2, pp. 227–238, 2014.

[15] R. Chandramouli, M. Kharrazi, and N. Memon, "Image steganography and steganalysis: concepts and practice", Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 2939, pp. 35–49, 2004.

[16] A. Martin, G. Sapiro, and G. Seroussi, "Is image steganography natural?", IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2040–2050, 2005.

[17] P. Singh and R. Chadha "A survey of digital watermarking techniques, applications and attacks", International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, no. 9, pp.165–175, 2013.

[18] V. Sabeti, S. Samavi, and S. Shirani, "An adaptive LSB matching steganography based on octonary complexity measure", Multimedia tools and applications, vol. 64, no. 3, pp. 777–793, 2013.

[19] V. Verma and R. Jha, "Improved watermarking technique based on significant difference of lifting wavelet coefficients", Signal, Image and Video Processing (SIViP), vol. 9, no. 6, pp. 1443–1450, 2015.

[20] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani "Steganalysis and payload estimation of embedding in pixel differences using neural networks", Pattern Recognition, vol. 43, no. 1, pp. 405–415, 2010.

[21] C. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various steganographic techniques used for information hiding", International

Journal of Computer Science and Engineering Survey (IJCSES), vol. 4, no. 6, pp. 9–25, 2014.

[22] KH. Jung and KY. Yoo, "High-capacity index based data hiding method", Multimedia Tools and Applications, vol. 74, no. 6, pp. 2179–2193, 2015.

[23] A. Khan, A. Siddiqa, S. Munib, and S. Malik, "A recent survey of reversible watermarking techniques", Information Sciences, vol. 279, pp. 251–272, 2014.

[24] J. Mielikainen, "LSB matching revisited", IEEE Signal Processing Letters, 2006, vol. 13, no. 5, pp. 285–287, 2006.

[25] NI. Wu, KC. Wu, and CM. Wang, "Exploring pixel-value differencing and base decomposition for low distortion data embedding", Applied Soft Computing, vol. 12, no. 2, pp. 942–960, 2012.

[26] X. Liao, Q. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", Journal of visual communication and image representation, vol. 22, no. 1, pp. 1–8, 2011.

[27] T. Sharp, "An implementation of key-based digital signal steganography", Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 2137, pp. 13–26, 2001.

[28] B. Li, J. He, J. Huang, and Y. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, 2011.

[29] Z. Xia, X. Wang, X. Sun, Q. Liu, and N. Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels", Multimedia Tools and Applications, vol. 75, no. 4, pp. 1947–1962, 2016.

[30] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol. 24, no. 9, pp.1613–1626, 2003.

[31] T. Mahjabin, S. Hossain, M. Haque, "A block based data hiding method in images using pixel value differencing and LSB substitution method". Proc. International Conference on Computer and Information Technology (ICCIT), Chittagong, Bangladesh, 2012, pp. 168–172.

[32] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing", IET image processing, vol. 6, no. 6, pp. 677–686, 2012.

[33] JK. Mandal and D. Das, "A novel invisible watermarking based on cascaded PVD integrated LSB technique", Communications in Computer and Information Science, Springer Berlin Heidelberg, vol. 305, pp. 262–268. 2012.

[34] C. Chang and H. Tseng, "A steganographic method for digital images using side match", Pattern Recognition Letters, vol. 25, no. 12, pp. 1431–1437, 2004.

[35] X. Li, B. Yang, D. Cheng, and T. Zeng, "A generalization of LSB matching", IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69–72, 2009.

[36] C. Wang, X. Li, B. Yang, X. and Lu, C. Liu, "A content-adaptive approach for reducing embedding impact in steganography". Proc. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, 2010, pp. 1762–1765.

[37] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited", IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 201–214, 2010.

[38] Y. Tsai, Y. Huang, R. Lin, and C. Chan, "An Adjustable Interpolation-based Data Hiding Algorithm Based on LSB Substitution and Histogram Shifting", International Journal of Digital Crime and Forensics, vol. 8, no. 2, pp. 48–61, 2016.

[39] N. Akhtar, "An LSB Substitution with Bit Inversion Steganography Method", Smart Innovation, Systems and Technologies, Springer India, vol. 43, pp 515–521, 2015.

[40] K. Jung and K. Yoo, "Steganographic method based on interpolation and LSB substitution of digital images", Multimedia Tools and Applications, vol. 74, no. 6, pp. 2143–2155, 2015.

[41] USC-SIPI Image Database. http://sipi.usc.edu/database/database.php. Accessed 17th September 2016.

[42] The University of Waterloo–Image repository. http://links.uwaterloo.ca/ Repository.html. Accessed 17th September 2016.

[43] M. Subhedar and V. Mankar, "Current status and key issues in image steganography: A survey", Computer Science Review, vol. 13, pp. 95–113, 2014.

[44] C. Lee and H. Chen, "A novel data hiding scheme based on modulus function", Journal of Systems and Software, vol. 83, no. 5, pp. 832–843, 2010.

[45] P. Gupta, R. Roy, and S. Changder, "A secure image steganography technique with moderately higher significant bit embedding". Proc. International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2014, pp. 1–6.

[46] O. Okman, and G. Akar, "Quantization index modulation-based image watermarking using digital holography", Journal of the Optical Society of America A, Optics, Image Science, and vision, vol. 24, no. 1, pp. 243–252, 2007.