

Article Generalized Scheme Based on Octagon-Shaped Shell for Data Hiding in Steganographic Applications

Hui-Shih Leng

Department of Mathematics, National Changhua University of Education, Changhua 50007, Taiwan; lenghs@cc.ncue.edu.tw

Received: 15 April 2019; Accepted: 29 May 2019; Published: 4 June 2019



Abstract: The exploiting modification direction scheme is a well-known data hiding method because of its high payload and low distortion. Its most criticized drawback is that the secret data must be converted to a non-binary numeral system before the embedding procedure. To overcome this drawback, one study proposed a turtle shell-based scheme for data hiding, in which a reference matrix was constructed based on a hexagon-shaped shell to embed three secret bits into each pixel group of a pair of pixels of the cover image. In a subsequent work, the embedding capacity was increased by using an octagon-shaped shell instead of a hexagon-shaped shell in the reference matrix. The above scheme was extended by utilizing a regular octagon-shaped shell in the reference matrix to reduce the distortion of the worst case. In another approach, the payload of the octagon-shaped-shell-based data hiding scheme was maximized by searching for the appropriate width and height of the octagon. In this study, we generalize the data hiding scheme based on an octagon-shaped shell so that the above-mentioned four schemes can be regarded as specific cases of the proposed method.

Keywords: exploiting modification direction scheme; turtle shell; octagon-shaped shell

1. Introduction

The popularity of computers and rapid growth of the internet makes digital data widely used all over the world. It is very convenient to easily share enormous multimedia data through ubiquitous channels. However, it also raises concerns regarding threats to consumers' personal privacy. Traditionally, Cryptology has been used as a reliable and safe method of transmission. However, the encrypted data may evoke suspicion from eavesdroppers. Data hiding techniques were invented to overcome this drawback by imperceptibly embedding secret data into a cover media (text, image, audio, or video) and satisfies the imperceptibility requirement. Once a cover media embeds the secret data, it becomes a stego-media. In this study, we use a grayscale image as the cover media. Data hiding can be broadly classified into two categories: reversible and irreversible. In some applications, such as military, medical, and astronomical imagery, besides the requirement of a high embedding capacity and visual quality of the stego-image, recovering a cover image without any distortion is also necessary. Reversible data hiding can restore the cover image after extracting the secret data from the stego-image, whereas irreversible data hiding cannot. However, irreversible data hiding is well-known because of its high payload and easy implementation.

The least significant bit (LSB) substitution scheme is a prominent irreversible data hiding scheme; it directly substitutes *n* secret bits into *n* LSBs of each pixel of the cover image. It achieves a high payload and a stego-image of good visual quality [1]. Two important strategies are applied to the LSB scheme for improving the visual quality of the stego-image: the optimal pixel adjustment process (OPAP) proposed by Chan and Cheng [2] and the modulus function proposed by Thien and Lin [3]. To overcome the asymmetry of an LSB, Li et al. proposed the LSB matching scheme (LSBM) [4]. Mielikainen proposed the LSB matching revisited scheme, in which one is added or subtracted from a



pixel pair of two consecutive secret bits [5]. However, the embedded secret data by the LSB scheme can be detected by RS-steganalysis [6].

To increase the resistance to steganalysis, Zhang and Wang proposed the exploiting modification direction (EMD) scheme [7]. The EMD scheme uses n pixels as a group to embed one secret digit in a (2n + 1)-ary numeral system, and it defines an extraction function to construct a hypercube as a reference to modify the cover pixels. In the EMD scheme, a maximum of one pixel in the group is increased or decreased by 1; therefore, it has a low distortion.



Figure 1. An example of the exploiting modification direction (EMD) scheme (n = 2).

For example, when n = 2 and the extraction function is defined as $f(x_1, x_2) = (1 \times x_1 + 2 \times x_2) \mod 5$, we can construct a hypercube as shown in Figure 1. Suppose $(x_1, x_2) = (3, 2)$ is a pixel pair of the cover image. If the to-be-embedded 5-ary secret digit is 0, 1, 2, 3, or 4, then we choose stego-pixels (3,1), (2,2), (3,2), (4,2), or (3,3), respectively.

There are two weaknesses to the EMD scheme. One is the limitation of the payload. To increase the payload, many researchers use two pixels as a group and define different extraction functions for the embedding and extraction procedures [8–13]. Chao et al. employed a diamond-shaped shell to embed a $(2k^2 + 2k + 1)$ -ary numeral system secret digit and increased the payload up to 2.68 bpp (k = 4) [8]. Kim et al. proposed the 2-EMD and EMD-2 schemes based on a log₂ (2 (5*n* – 7) + 1)-ary numeral system secret digit and achieved a maximum payload of log₂ (10) bpp (about 3.22 bpp) [9]. Kieu and Chang improved the EMD scheme by using eight modification directions on a square-shaped shell of size *s* × *s* and attained a maximum payload of up to 4.5 bpp (*s* = 23) [10]. Kim used a codebook to embed a $(2^{n+x} - 1)$ -ary numeral system secret digit and achieved a maximum payload of 2.5 bpp [12]. Leng and Tseng extended the EMD scheme on a three-dimensional (3D)-hypercube sized $w \times w \times w$ and generalized the EMD scheme on an *n*-dimensional hypercube with a maximum payload of up to 4.75 bpp (w = 27) [13].

Another shortcoming of the EMD scheme is that the secret data must be converted to a non-binary numeral system. To overcome this issue, Chang et al. proposed a novel turtle-based data hiding scheme. In this, a reference matrix is constructed based on a hexagon-shaped shell to embed three secret bits in each pixel pair of the cover image [14]. It achieved a payload of 1.5 bpp with a high visual quality of the stego-image (about 49.42 dB). Kurup et al. proposed a data hiding scheme based on an octagon-shaped shell to embed four secret bits in the cover pixel pairs and achieved a payload of 2 bpp [15]. Subsequently, Leng improved the scheme of Kurup et al. by using a regular octagon-shaped shell to embed five secret bits in the cover pixel pairs and realized a payload of 2.5 bpp [16]. In addition, this scheme has the best combination of a high payload and low distortion. Leng and Tseng extended the scheme of Leng to maximize the payload of the octagon-shaped-shell-based data hiding scheme and achieved a payload of 3.5 bpp with a stego-image of a good visual quality (about 30.61 dB) [17].

In this study, we consider the size of an octagon-shaped shell. The proposed method generalizes the data hiding scheme based on an octagon-shaped shell in the reference matrix. Therefore, the schemes of Kurup, Leng, and Leng and Tseng can be regarded as specific cases of the proposed method.

The remainder of this paper is organized as follows. Section 2 reviews the schemes of Chang et al., Kurup et al., and Leng. Section 3 describes the proposed method. The experimental results are given in Section 4. Finally, Section 5 draws the conclusions.

2. Related Works

In this section, the schemes of Chang et al., Kurup et al., and Leng are introduced briefly. According to the scheme of Chang et al., a reference-matrix-based data hiding scheme is used in the embedding and extraction procedure. First, a reference matrix with a size of 256×256 is constructed for the grayscale cover image in the embedding and extraction procedure. Then, the cover image is divided into pixel pairs of two neighbor pixels. For each pixel pair (x_1,x_2) , the location of M (x_1,x_2) determines the to-be-embedded secret digits. To embed the secret digit, *s*, into the pixel pair, (x_1,x_2) , the pixel pair is first located in the reference matrix, M, as M (x_1,x_2) , and the element, M (x_1',x_2') , which has the shortest distance with M (x_1,x_2) and M $(x_1',x_2') = s$, is searched. Subsequently, the original pixel pair, (x_1,x_2) , is modified to (x_1',x_2') . In the extraction procedure, the secret digit is extracted correctly from the stego pixel pair that is mapped to the element, M (x_1',x_2') , in the reference matrix, M.

2.1. Scheme of Chang et al.

In the scheme of Chang et al., the reference matrix is composed of numerous contiguous hexagons called turtle shells, where each hexagon contains eight different digits ranging from 0 to 7, which include two back digits and six edge digits. For each pixel pair, the scheme of Chang et al. embeds three secret bits. The construction of the reference matrix is based on two rules. The value difference between two adjacent columns in the same row is set as 1, and the value between two adjacent rows in the same column is set alternately as +2 and +3. Figure 2 illustrates an example of a reference matrix, M, based on hexagon-shaped shells.



Figure 2. Reference matrix M of the scheme of Chang et al.

For example, a cover pixel pair, (3,4), and the to-be-embedded secret bits are $(111)_2 = 7$. The cover pixel pair, (3,4), is mapped to M (3,4) = 3 in the reference matrix, M. Then, the candidate stego pixel pairs, M (1,5) = 7, M (2,2) = 7, M (4,5) = 7, and M (5,3) = 7, choose (4,5) as the stego pixel pair to ensure the lowest distortion. In the extraction procedure, if M (4,5) = 7 = $(111)_2$; then, the secret digits are extracted correctly.

The scheme of Chang et al. makes an important contribution in that it overcomes the drawback of the tradition EMD scheme of converting the secret data into a non-binary numeral system before the embedding and extraction. The construction of the reference matrix has become a new topic in data hiding.

2.2. Scheme of Kurup et al.

0

1

2

3 4

In the scheme of Kurup et al., the reference matrix is constructed based on the concept of octagon shells. The octagon-shaped shells contain 16 different digits ranging from 0 to 15, including six back digits and ten edge digits. For each pixel pair, the scheme of Kurup et al. embeds four secret bits. The construction of the reference matrix is based on two rules. The value difference between two adjacent columns in the same row is set as 1, and the value between two adjacent rows in the same column is set alternately as +4, +5, and +4. Figure 3 illustrates an example of a reference matrix, M, based on octagon-shaped shells.

5 6 7

8 9

r.

| | | 0 | - | - | 2 | • | 2 | 0 | , | 0 | 2 | |
|-------|----------|----|--------------|----------|-----|--------------|----|-----|-----|----|----|------|
| 0 | | 0 | x | -2- | -3 | 4 | 5 | 6 | 7 | 8 | 9 | |
| 1 | 24 | 4 | 5 | 6 | 7 | F | 9 | 10 | 11 | 12 | 13 | |
| 2 |] | ٩ | 10 | 11 | 12 | 13 | 14 | 15 | 0 | | 2 | |
| 3 | | 13 | À | ₽ | Þ | 1 | ¥ | 3 | ¥ | 5 | 6 | |
| 4 | 24 | Ţ | 2 | 3 | 4 | ¥ | 6 | 7 | 8 | 2 | 10 | |
| 5 | | é | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | |
| 6 | | 10 | \mathbf{i} | 12 | × | 14 | ¢, | 0 | ¥ | 2 | 3 | |
| 7 | | 14 | 15 | 0 | 1 | \mathbf{A} | 3 | 4 | 5 | 0 | 7 | |
| 8 | | 1 | 4 | 5 | 6 | 大 | 8 | 9 | 10 | цı | 12 | |
| 9 | 1 | 7 | 8 | 9 | -10 | 11 | 12 | -13 | -14 | 15 | 0 | |
| : | | | | | | | | | | | | |
| x_1 | ¥ | | | | | | | | | | | |

Figure 3. Reference matrix, M, of the scheme of Kurup et al.

For example, a cover pixel pair (4,2) and the to-be-embedded secret bits are $(1011)_2 = 11$. The cover pixel pair, (4,2), is mapped to M (4,2) = 3 in the reference matrix, M. Then, the candidate stego pixel pairs are M (2,2) = 11, M (5,5) = 11, and M (6,1) = 11, and (2,2) is selected as the stego pixel pair to ensure the lowest distortion. In the extraction procedure, if M (2,2) = 11 = $(1011)_2$, then the secret digit can be extracted correctly.

It is trivial that based on the reference matrix, the schemes of Chang et al. and Kurup et al. have the same embedding and extraction procedure; the only difference is in the method to construct the reference matrix for the trade-off between the payload and visual quality of the stego-image.

2.3. Scheme of Leng

In the scheme of Kurup et al., if the octagon-shaped shell is not regular, then the worst case will decrease the distortion. The scheme of Leng summarizes this problem as Equation (1),

$$n^2 - 4 = 2^k \tag{1}$$

where *n* is the octagon size, *k* is a positive integer, and $1 \le k \le 8$.

In the scheme of Leng, the reference matrix is constructed based on the concept of regular octagon shells. It denotes n = 6 and k = 5 and then constructs a regular octagon-shaped shell reference matrix. For each pixel pair, the scheme of Leng embeds five secret bits. The construction of the reference matrix is based on two rules. The value difference between two adjacent columns in the same row is set as 1, and the value between two adjacent rows in the same column is set alternately as +5, +6, +6, and +5. Figure 4 illustrates an example of reference matrix M, based on regular octagon-shaped shells.

| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | x_2 |
|-------|----|----|----------------|-----|----|------------|------------|--------------------|----|----|----------------|----------------|----|-----------|
| | | | | | | | | | | | | | | → |
| 0 | 2 | 0 | V | 2 | 3 | ¥ | 5 | 6⁄ | 7 | 8 | 9 | 10 | 11 | |
| 1 | | 5/ | 6 | 7 | 8 | 9 | \$ | 11 | 12 | 13 | 14 | ¥2 | 16 | |
| 2 | ٩ | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | |
| 3 | ۲ | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | |
| 4 | | 23 | 2 4 | 25 | 26 | 27 | 28 | No. | 30 | 31 | 0/ | $\overline{1}$ | 2 | |
| 5 | | 28 | 29 | -30 | 31 | \diamond | 1 | $\hat{\mathbf{A}}$ | \$ | 4 | <5 | 6 | 7 | |
| 6 | | 1 | $\overline{2}$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| 7 | Ĭ) | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | |
| 8 | | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | |
| 9 | | 19 | 20 | 21 | 22 | 23 | $\sqrt{4}$ | 25 | 26 | 27 | 28 | 29 | 30 | |
| 10 | S. | 24 | 25 | -26 | 27 | 28 | 29 | 30 | 31 | 0 | $\overline{1}$ | 2 | 3 | |
| 11 | | 29 | 30 | 31 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | |
| : | | | | | | | | | | | | | | |
| x_1 | ¥ | | | | | | | | | | | | | |

Figure 4. Reference matrix (n = 6 and k = 5) of the scheme of Leng.

For example, a cover pixel pair is (6,7) and the to-be-embedded secret bits are $(10111)_2 = 23$. The cover pixel pair, (6,7), is mapped to M (6,7) = 8 in the reference matrix, M. Then, the candidate stego pixel pairs are M (3,6) = 23, M(6,10) = 23, and M (9,4) = 23, and (3,6) is selected as the stego pixel pair to ensure the lowest distortion. In the extraction procedure, if M $(3,6) = 23 = (10111)_2$, then the secret digits can be extracted correctly.

The scheme of Leng constructs reference-matrix-based data hiding with the best balance between the payload and visual quality of the stego-image.

3. The Proposed Method

In the section, we generalize the data hiding scheme based on octagon-shaped shells. We improve Equation (1) as Equation (2),

$$m \cdot n - 4 \cdot \frac{k(k+1)}{2} = 2^w \tag{2}$$

where *m* and *n* are the width and height of an octagon (m \leq n), respectively, *k* is the width and height of the octagon ($k \leq \left| \frac{m}{2} \right|$), respectively, and *w* is a positive integer (1 $\leq w \leq$ 8).



Figure 5. Reference matrix of the proposed method.

In addition, we demand that this octagon-shaped shell contains 2^w different digits ranging from 0 to $2^w - 1$ digits. Then, for each pixel pair, the proposed method embeds w secret bits. The construction of reference matrix M, sized 256×256 , is based on the following three rules. Let $M = (a_{i,j})_{256 \times 256}$; then, element $a_{0,0}$ can choose any number from the range $[0,2^w-1]$ and serve as a key. The value difference between two adjacent columns in the same row is set as 1, and the value between the two adjacent rows is set alternately as $d_0, d_1, d_2, \ldots, d_{m-1}$, where d_i is defined as follows:

| $d_0 = a_{0,0}, d_i = a_{i+1,0} - a_{i,0}$ | $0 \le i \le m - 1$ |
|---|-----------------------|
| $d_i = d_{i-1} + (n-2 k+1 - i + 1)$ | $1 \le i \le k$ |
| $d_i = d_{i-1} + (n-2 m-1-k -i +1)$ | $m-k \le i \le m-1$ |
| $d_i = d_{i-1} + n$ | $k+1 \le i \le m-1-k$ |

Figure 5 illustrates an example of the reference matrix, M, of the proposed method.

Notice that we suppose $m \le n$; if m > n, then the reference matrix is different but the payload and quality of the stego-image are the same. For example, (m,n,k,w) = (3,4,1,3) and (m,n,k,w) = (4,3,1,3) are illustrated in Figure 6.



Figure 6. Reference matrices of (*m*,*n*,*k*,*w*) = (3,4,1,3) and (*m*,*n*,*k*,*w*) = (4,3,1,3).

Based on Figure 5, we obtain all the solutions of Equation (2). There are 29 solutions: 14 solutions for k = 1, three solutions for k = 2, seven solutions for k = 3, one solution for k = 4, one solution for k = 6, two solutions for k = 7, and one solution for k = 8.

The distortion of a stego-image is determined by the longest distance of the reference matrix. In the embedding procedure, for each cover pixel pair (x_1,x_2) , if the to-be-embedded secret digits are s, then the element M (x_1',x_2') , which has the shortest distance with M (x_1,x_2) and M $(x_1',x_2') = s$, is searched. In the extraction procedure, the secret digit is extracted correctly from the stego pixel pair, which is mapped to the element, M (x_1',x_2') , in the reference matrix, M.

From Table 1, we denote (m,n,k,w) = (3,4,1,3), and in Figure 7b, we reconstruct the reference matrix by hexagon-shaped shells to compare with the scheme of Chang et al. (Figure 2). This achieves the same payload and visual quality of the stego-image of the scheme of Chang et al. In addition, the scheme of Kurup et al. is the case of (m,n,k,w) = (6,6,1,5), the scheme of Leng scheme is the case of (m,n,k,w) = (6,6,1,5), and that of Leng and Tseng is the case of (m,n,k,w) = (11,12,1,7).

| | <i>k</i> = 1 | <i>k</i> = 2 | <i>k</i> = 3 | k = 4 | <i>k</i> = 6 | <i>k</i> = 7 | <i>k</i> = 8 |
|-----------|--|-------------------------------------|---|-----------|--------------|-------------------------|--------------|
| (m,n,w) | $(3,4,3)^1,$ (3,12,5), (3,44,7), $(4,5,4)^2,$ (4,9,5), (4,17,6), (4,33,7), (4,65,8), (5,52,8), $(6,6,5)^3,$ (6,22,7), (10,26,8), $(11,12,7)^4,$ (13,20,8) | (5,28,7), (7,20,7), (10,14,7) | (7,8,5), (7,40,8), (8,11,6), (8,19,7), (8,35,8), (10,28,8), (14,20,8) | (12,14,7) | (17,20,8) | (15,16,7), (16,23,8) | (20,20,8) |
| solutions | 14 | 3 | 7 | 1 | 1 | 2 | 1 |

Table 1. All the solutions of the proposed method.

¹ Scheme of Chang et al. is the case of (m,n,k,w) = (3,4,1,3). ² Scheme of Kurup et al. is the case of (m,n,k,w) = (4,5,1,4). ³ Scheme of Leng is the case of (m,n,k,w) = (6,6,1,5). ⁴ Scheme of Leng and Tseng is the case of (m,n,k,w) = (11,12,1,7).

| 0 | /+ | * | 3 | 1 | 5 | 6 | 7 | | 0 | 0 | <u>_</u> 1> | 2 | 3 | 4 | <u>^</u> \$~ | 6 | 7 |
|-----------|------------|----------|---|----------------|---|---|---|--|---|----|-------------|---|-------------|---------|--------------|------------|---|
| <u>s</u> | 4 | 5 | X | 7 | 0 |) | 2 | | 1 | 3 | 4 | 4 | 6 | 1 | Ø | 1 | 2 |
| 6 | >7- | -0 | 1 | \geq_2 | | 4 | 5 | | 2 | 6. | 7 | Å | 1 | | 3 | | 5 |
| \langle | 2 | 3 | X | \odot | 6 |) | 0 | | 3 | 1 | ¥ | 3 | Y | \odot | K | 7 | Þ |
| 4 | >> | -64 | 7 |) . | 1 | 2 | 3 | | 4 | 4 | X | 6 | X | 0 | | 2 | В |
| \langle | 0 | 1 | X | 3 | 4 | > | 6 | | 5 | 1 | 0 | Y | 2 | Y | 4 | \searrow | 6 |
| 2 | <u>\</u> 3 | 42 | 5 | <u>\</u> 6- | | 0 | 1 | | 6 | 2 | 3 | J | 5 | 6 | 7 | þ | 1 |
| 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | | 7 | 5 | 6 | 7 | \0 ^ | 1 | \searrow | 3 | 4 |
| | | | | | | | | | | | | | | | | | |

Figure 7. Reference matrix (**a**) of the proposed method with (m,n,k,w) = (3,4,1,3) (**b**) reconstructed by hexagon-shaped shells to compare with the scheme of Chang et al.

4. Results and Discussion

In the experiment, six 512×512 grayscale images: Tiffany, Baboon, Lena, Jet, Scene, and Peppers, were chosen from the SIPI image database; they are adopted as the cover image and illustrated in Figure 8. Random secret bits are used in the following experiments.

(a)

Figure 8. Six 512 × 512 grayscale images (a) Tiffany (b) Baboon (c) Lena (d) Jet (e) Scene (f) Peppers.

The performance of the stego-image is measured by the peak signal to noise ratio (PSNR). The PSNR and mean square error (MSE) are defined as follows:

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE}$$
(3)

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(x_{i,j} - x_{i,j'} \right)^2$$
(4)

where M and N are the length and width of the cover image, respectively, $x_{i,j}$ and $x_{i,j}'$ are the pixel values of the cover image and stego-image, respectively. Table 2 present the PSNR values of the proposed method as a function of the payloads (w = 3, 4, 5, 6, 7, and 8).

Table 2. Performance of the proposed method.

| (<i>m</i> , <i>n</i> , <i>k</i>) | w = 3 | (<i>m</i> , <i>n</i> , <i>k</i>) | w = 4 | (<i>m</i> , <i>n</i> , <i>k</i>) | <i>w</i> = 5 | (<i>m</i> , <i>n</i> , <i>k</i>) | <i>w</i> = 6 | (<i>m</i> , <i>n</i> , <i>k</i>) | <i>w</i> = 7 | (<i>m</i> , <i>n</i> , <i>k</i>) | <i>w</i> = 8 |
|------------------------------------|-----------------------|---|-----------------------|---|---|--|--------------------------------|--|--|---|---|
| (<i>m,n,k</i>) (3,4,1) | <i>w</i> = 3 49.74 | (<i>m</i> , <i>n</i> , <i>k</i>) (4,5,4) | <i>w</i> = 4 46.82 | (<i>m,n,k</i>) (3,12,1) (4,9,1) (6,6,1) (7,8,3) | w = 5 41.34 43.14 43.94 43.31 | (<i>m,n,k</i>) (4,17,1) (8,11,3) | <i>w</i> = 6 37.95 40.71 | (<i>m,n,k</i>) (3,44,1) (4,33,1) (6,22,1) (11,12,1) (5,28,2) (7,20,2) (10,14,2) | w = 7 29.05 31.83 35.17 37.83 34.02 36.49 37.77 | (<i>m,n,k</i>) (4,65,1) (5,52,1) (10,26,1) (13,20,1) (7,40,3) (8,35,3) (10,28,3) | w = 8 25.05 = 27.28 33.05 34.40 30.79 31.96 33.45 |
| | | | | | | | | (8,19,3) | 37.23 | (14,20,3) | 34.70 24.51 |
| | | | | | | | | (12,14,4) (15,16,7) | 36.49 | (17,20,8) (16,23,7) (20,20,8) | 34.51 33.79 |

When w = 3, the payload is 1.5 bpp, and there is only one case. Compared to the scheme of Chang et al. (49.42 dB), the proposed method provides a better image quality (49.74 dB) with the same

payload (1.5 bpp), because the octagon-shaped shells can better complete coverage the reference matrix. When w = 4, the payload is 2 bpp, and there is only one case. The case (m,n,k) = (4,5,4) is the same as the scheme of Kurup et al. When w = 5, the payload is 2.5 bpp and there are four cases. The case (m,n,k) = (6,6,1) is the same as that of the scheme of Leng. It has the highest image quality because its m value is closer to the n value, i.e., the octagon-shaped shell is closer to the circle shape so that it causes less distortion. When w = 6, the payload is 3 bpp, and there are two cases. For the same reason as described above, the case (m,n,k) = (8,11,3) has a better image quality than the case (m,n,k) = (4,17,1). When w = 7, the payload is 3.5 bpp, and there are ten cases. The case (m,n,k) = (11,12,1) is the same as that of the scheme of Leng and Tseng. In the case (m,n,k) = (3,44,1), the m value is extremely far from the n value, such that it causes a large distortion. In addition, if the pixel pair M (x_1,x_2) is located in the border area of the reference matrix, it causes a large distortion when it searches the element, M $(x_1',x_2') = s$. When w = 8, the payload is 4 bpp and there are eleven cases. Similarly, the cases (m,n,k) = (4,65,1) and (m,n,k) = (5,52,1) are two poor cases. However, the case (m,n,k) = (14,20,3) achieves a high payload (4 bpp) with a good visual stego-image quality (34.70 dB).

The proposed method improves Equation (1) as Equation (2) and generalizes the data hiding scheme based on an octagon-shaped shells. The reason why the proposed method achieves better performance is because the octagon-shaped shells can better complete coverage of the reference matrix. Table 2 shows that the proposed method can provide various hiding capacities (i.e., parameter (m,n,k)) with good and acceptable visual qualities to satisfy different requirements of users.

5. Conclusions

In this study, the proposed method is based on the concept of using a reference matrix. The proposed method also improves the scheme of Leng to generalize the data hiding scheme based on octagon-shaped shells. Therefore, the schemes of Chang et al., Kurup et al., Leng, and Leng and Tseng can be regarded as specific cases of the proposed method. The payload and image quality depend on the width and height of both the octagon and the corner of the octagon. If the value *m* is close to the value *n* then the octagon-shaped shell is close to a circle shape and will cause less distortion. Contrastingly, if the pixel pair $M(x_1,x_2)$ is located in the border area of the reference matrix, it causes a large distortion when it searches the element $M(x_1',x_2') = s$. In the future, we plan to improve Equation (2) so that the number of digits contains in an octagon-shape shells is $m \times n$ instead of 2^w .

Conflicts of Interest: The authors declare no conflict of interest.

References

- 1. Tuner, L.F. Digital Data Security System. Patent IPN WO 89/08915, 21 September 1989.
- Chan, C.-K.; Cheng, L. Hiding data in images by simple LSB substitution. *Pattern Recognit.* 2004, 37, 469–474. [CrossRef]
- 3. Thien, C.-C.; Lin, J.-C. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. *Pattern Recognit.* **2003**, *36*, 2875–2881. [CrossRef]
- 4. Li, X.; Yang, B.; Cheng, D.; Zeng, T. A generalization of LSB matching. IEEE Signal Proc. Lett. 2009, 16, 69–72.
- 5. Mielikainen, J. LSB matching revisited. IEEE Signal Proc. Lett. 2006, 13, 285–287. [CrossRef]
- Fridrich, J.; Goljan, M.; Du, R. Reliable Detection of LSB Steganography in Color and Grayscale Images. In Proceedings of the 2001 Workshop on Multimedia and Security New Challenges, Ottawa, ON, Canada, 5 October 2001.
- 7. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **2006**, *10*, 781–783. [CrossRef]
- Chao, R.-M.; Wu, H.-C.; Lee, C.-C.; Chu, Y.-P. A novel image data hiding scheme with diamond encoding. EURASIP J. Inf. Sec. 2009, 2009, 1–9. [CrossRef]
- Kim, H.; Kim, C.; Choi, Y.; Wang, S.; Zhang, X. Improved modification direction methods. *Comput. Math. Appl.* 2010, 60, 319–325. [CrossRef]

- Kieu, T.D.; Chang, C.-C. A steganographic scheme by fully exploiting modification directions. *Expert Syst. Appl.* 2011, 38, 10648–10657. [CrossRef]
- 11. Kim, C. Data hiding by an improved exploiting modification direction. *Multimed. Tools Appl.* **2012**, *69*, 569–584. [CrossRef]
- 12. Liu, Y.; Chang, C.-C.; Huang, P.-C. Extended Exploiting-Modification-Direction Data Hiding with High Capacity. In Proceedings of the International Conference on Video and Image Processing—ICVIP 2017, Singapore, 27–29 December 2017.
- 13. Leng, H.-S.; Tseng, H.-W. Generalize the EMD scheme on an *n*-dimensional hypercube with maximum payload. *Multimed. Tools Appl.* **2019**, 1–15. [CrossRef]
- Chang, C.C.; Liu, Y.; Nguyen, T.S. A Novel Turtle Shell Based Scheme for Data Hiding. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, Japan, 27–29 August 2014.
- Kurup, S.; Rodrigues, A.; Bhise, A. Data hiding scheme based on octagon shaped shell. In Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kerala, India, 10–13 August 2015.
- Leng, H.-S. Data Hiding Scheme Based on Regular Octagon-Shaped Shells. In Proceedings of the Advances in Intelligent Information Hiding and Multimedia Signal Processing Smart Innovation, Systems and Technologies, Kaohsiung, Taiwan, 21–23 November 2017.
- Leng, H.-S.; Tseng, H.-W. Maximizing the payload of the octagon-shaped shell-based data hiding scheme. In Proceedings of the 2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST), Taichung, Taiwan, 8 November 2017.



© 2019 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).