Reversible Data Hiding Scheme Based on Fully Exploiting the Orientation Combinations of Dual Stego-images

Xiaofeng Chen[1,2] and Wenlong Guo[1]

(Corresponding author: Xiaofeng Chen)

School of Electronic Information Science, Fujian Jiangxia University[1]

Digital Fujian, Internet-of-Things Key Lab of Information Collection and Processing in Smart Home[2]

Fuzhou 350108, China

(Email: dragon_ball@fjjxu.edu.cn)

(Received Aug. 4, 2018; Revised and Accepted Dec. 7, 2018; First Online Mar. 2, 2019)

Abstract

In order to increase the embedding capacity and achieve good visual quality, this paper proposes a novel reversible data hiding scheme based on fully exploiting the combinations of pixel pair orientations in two stego-images. We labelled these combinations from 0 to 24, each combination representing for embedding a base-25 digit. The embedding capacity of the proposed scheme is approximate to 1.14 bit per pixel (bpp). Since the modification of the cover pixel value is tiny, the two generated stego-images also have a good visual quality of 49.92 dB. Moreover, not any overhead messages are required in this scheme. In the experiment, the proposed scheme outperforms some state-of-the-art methods in terms of measuring in embedding ratio (ER) or peak-signal-to-noise ratio (PSNR). In addition, the proposed scheme has good performance on resisting static attacks on pixel-value differencing (PVD) histogram.

Keywords:Dual Stego-images; Orientation Combinations; Reversible Data Hiding (RDH)

1 Introduction

With the fast development of the Internet, one can transmit information to communicate with people around the world simply by a few clicks or touches on the screen. However, due to the public nature of the network, our transmitted messages can be easily stolen or destroyed by attackers. The most of our concern is focused on enhancing the security of the transmitted data. Cryptography is a traditional method for protecting the confidential data. It will encrypt the to-be-transmitted data into ciphertext by a secret key. The receiver who has the secret key can decrypt the ciphertext to obtain the secret data [11]. Yet, the data after encryption remain out there where they are in a meaningless state that will attract the attention of illegal users. Data hiding is an alternative technique which can conceal the confidential information into a to-be-transmitted image which is referred to as a cover image to obtain a stego-image. Since the difference between the cover image and the stego-image is very small, the human eyes can't tell whether the stego-image contains the secret information or not.

Data hiding can be divided into two categories, *i.e.*, irreversible data hiding [3–5,15,20,21,28,29] and reversible data hiding (RDH) [1,6,10,12,14,16,22,25–27]. The difference between them depends on whether the cover image can be retrieved from the stego-image or not [13]. Numerous RDH methods have been introduced and have been successful in some lossless applications such as military communications and medical cares. Among these RDH methods, difference expansion (DE) [26] and histogram-shift (HS) [22] are the two earliest major techniques. DE was first proposed by Tian in 2003 [26] which calculated the difference of two consecutive pixel values, doubled the result and concealed one secret bit into it. In 2006, Ni [22] first introduced the HS based technique that generated a histogram based on the frequency of each pixel value. The secret data were then embedded into the bin with the highest frequency.

Besides the DE and HS methods which embedded the secret data into the cover image to generate one stego-image, secret sharing [2,24] divided the secret data into n parts and concealed each part into the same cover image to obtain n stego-images. The secret data can be retrieved by the corporation of k or more stego-images, while insufficient number of stego-images can cause the leak of any information about the secret. Dual-image hiding techniques [8,9,17–19,23] can be considered as a special case of the secret sharing when k=2 and n=2. The secret data would not be obtained without two stego-images being processed simultaneously.

Dual image technology has attracted a lot of attention

in recent years. In 2007, Chang *et al.* [8] was pioneered in developing a reversible data hiding scheme by using two steganographic images. In their method, the secret data was first converted into a base-5 numeral system. Then each pixel pair of the cover image was modified to embed two base-5 digits according to the exploiting modification direction (EMD) magic matrix [29]. After processing the whole pixel pair in cover image, two stego-images were obtained. The capacity of their method is almost 1 bit per pixel (bpp) and the quality of generated stego-images can reach 45 dB.

In 2009, Lee *et al.* [18] considered each pixel pair as the center point and embedded two consecutive of two secret bits using the four directions of it to obtain the stego-pixel pair of the two stego-images. In order to implement the reversibility, the orientation relationship between the pixel pairs of the two images was utilized to determine whether the second two secret bits could be concealed in the second stego-pixel pair or not. Though the quality of two setgo-images could reach up to 52 dB, but the payload was no more than 0.75 bpp because only half of the whole orientation relationship could be used for embedding four secret bits.

In 2013, Lee and Huang [17] proposed a novel dual stego-images hiding scheme to increase the embedding capacity. They first converted the secret data into base-5 secret symbols by enhancing base-5 numeral system, every two secret symbols were considered as a set to embed in the identical cover pixel pair to obtain the stego-pixel pair through pre-defined embedding rules. Their embedding capacity was improved to 1.07 bpp.

In 2018, Liu and Chang [19] proposed a dual image hiding scheme based on turtle shell reference matrix. Each pixel in the cover image is duplicated to a pixel pair first. Three secret bits will be embedded when the pixel pair belongs to the back element and only one secret bit will be concealed in the edge type element of the cover pixel pair to obtain two stego-pixel value. The quality of the first stego-image can reach up to 51 dB while the second one can remain at 45 dB and the embedding capacity is almost 1 bpp.

In this paper, we proposed dual image hiding scheme to increase the embedding capacity and exploit the 25 orientation combinations in two stego-pixel pairs to achieve the reversibility. After labelling these combinations from 0 to 24, each combination can represent to embed a base-25 digit into a cover pixel pair. The image quality evaluated by peak-signal-to-noise ratio (PSNR) can reach up to 49.9 dB and the pure payload is around 1.14 bpp. Moreover, the proposed scheme has good performance for resisting static attacks of pixel-value differencing (PVD) histogram.

The rest of this paper is organized as follows. Section 2 describes the method proposed by Lee and Huang, and Section 3 then introduces the proposed scheme. Section 4 summarizes the experimental results and conclusions drawn can be found in Section 5.

2 Review of Lee and Huang's Method

Inspired by the EMD method introduced by Zhang and Wang in [29], Lee and Huang [17] proposed a reversible data hiding scheme by using the orientation combinations of dual stego-images. Pick up a pixel pair (x, y) from cover image, it can be mapped into a two-dimensional space. Each pixel value is ranging from 0 to 255 while the grayscale value is an 8-bits pixel intensity. Furthermore, the first dimension x represents the coordinate value in X-axis and the second dimension y represents the coordinate value in Y-axis. The pixel pair (x, y) is modified to (x_1, y_1) to embed a base-5 digit $m1$, and the other pixel pair (x_2, y_2) will be gained for embedding the second base-5 digit $m2$. When the secret data embedding procedure is implemented, two corresponding stego-images are both constructed. The embedding algorithm is described as below.

The original pixel pair is modified, according to the first pattern, to be the first pixel (x_1, y_1) for embedding $m1$. The value of (x_1, y_1) depends on the value of $m1$, as shown in Figure 1. Once the first secret digit is hidden, $m2$ can be concealed by modifying the original pixel pair according to the second pattern to produce the second pixel pair (x_2, y_2), as shown in Figure 1. The second pattern chosen to embed $m2$ depends on the value of $m1$. For example, if $m1$=3, then the second pattern marked as $P3$ will be selected to conceal $m2$. After the second pattern is determined, the value of (x_2, y_2) will be gained by the value of $m2$.

To explain this algorithm in more details, the embedding rules are created as shown in Table 1. It should be noticed that the overflow and underflow problem will arise in these embedding rules. Since the difference value of d_x (calculated by d_x=x_1-x_2) and d_y (calculated by d_x=y_1-y_2) all range from -2 to 2, Lee and Huang [17] set (x_1, y_1) equal to (x, y) and d_x=3 (or -3) or d_y=3 (or -3) when the overflow and underflow problem occurs.

When two stego-images are acquired, the sequential base-5 digit and the cover image can be retrieved by the following way.

1) Generate the extracting rules as shown in Table 2.

2) Pick up pixel pairs (x_1, y_1) and (x_2, y_2) from the first and the second stego-images, respectively. Calculate the value of d_x and d_y. The two embedded base-5 digits and the cover pixel pair can be determined by Table 2 directly.

3) If d_x or d_y equals to 3 (or -3), these mean that overflow and underflow has occurred. For these situations, no secret data is embedded and the cover pixel value equals to (x_1, y_1).

According to what's mentioned above, the embedding secret data and the cover image can be retrieved without any error. While enhancing the base-5 numeral system,

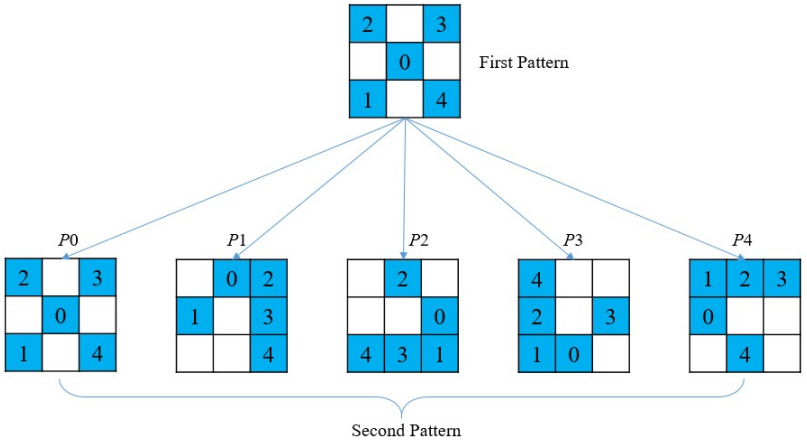

Figure 1: The first pattern and the five second patterns are marked as $P0$, $P1$, $P2$, $P3$ and $P4$

Table 1: The embedding rules of Lee and Huang's method

$m1$	(x_1, y_1)	$m2$	(x_2, y_2)
0	(x,y)	0	(x,y)
		1	$(x\text{-}1,y\text{-}1)$
		2	$(x\text{-}1,y\text{+}1)$
		3	$(x\text{+}1,y\text{+}1)$
		4	$(x\text{+}1,y\text{-}1)$
1	$(x\text{-}1,y\text{-}1)$	0	$(x,y\text{+}1)$
		1	$(x\text{-}1,y)$
		2	$(x\text{+}1,y\text{+}1)$
		3	$(x\text{+}1,y)$
		4	$(x\text{+}1,y\text{-}1)$
2	$(x\text{-}1,y\text{+}1)$	0	$(x\text{+}1,y)$
		1	$(x\text{+}1,y\text{-}1)$
		2	$(x,y\text{+}1)$
		3	$(x,y\text{-}1)$
		4	$(x\text{-}1,y\text{-}1)$
3	$(x\text{+}1,y\text{+}1)$	0	$(x,y\text{-}1)$
		1	$(x\text{-}1,y\text{-}1)$
		2	$(x\text{-}1,y)$
		3	$(x\text{+}1,y)$
		4	$(x\text{-}1,y\text{+}1)$
4	$(x\text{+}1,y\text{-}1)$	0	$(x\text{-}1,y)$
		1	$(x\text{-}1,y\text{+}1)$
		2	$(x,y\text{+}1)$
		3	$(x\text{+}1,y\text{+}1)$
		4	$(x,y\text{-}1)$

Table 2: The exacting rules of Lee and Huang's method

d_x	d_y	$m1$	$m2$	(x, y)
2	2	3	1	$(x_1\text{-}1,y_1\text{-}1)$
	1	3	2	$(x_1\text{-}1,y_1\text{-}1)$
	0	3	4	$(x_1\text{-}1,y_1\text{-}1)$
	-1	4	0	$(x_1\text{-}1,y_1\text{+}1)$
	-2	4	1	$(x_1\text{-}1,y_1\text{+}1)$
1	2	3	0	$(x_1\text{-}1,y_1\text{-}1)$
	1	0	1	(x_1,y_1)
	0	4	4	$(x_1\text{-}1,y_1\text{+}1)$
	-1	0	2	(x_1,y_1)
	-2	4	2	$(x_1\text{-}1,y_1\text{+}1)$
0	2	2	4	$(x_1\text{+}1,y_1\text{-}1)$
	1	3	3	$(x_1\text{-}1,y_1\text{-}1)$
	0	0	0	(x_1,y_1)
	-1	1	1	$(x_1\text{+}1,y_1\text{+}1)$
	-2	4	3	$(x_1\text{-}1,y_1\text{+}1)$
-1	2	2	3	$(x_1\text{+}1,y_1\text{-}1)$
	1	0	4	(x_1,y_1)
	0	2	2	$(x_1\text{+}1,y_1\text{-}1)$
	-1	0	3	(x_1,y_1)
	-2	1	0	$(x_1\text{+}1,y_1\text{+}1)$
-2	2	2	1	$(x_1\text{+}1,y_1\text{-}1)$
	1	2	0	$(x_1\text{+}1,y_1\text{-}1)$
	0	1	4	$(x_1\text{+}1,y_1\text{+}1)$
	-1	1	3	$(x_1\text{+}1,y_1\text{+}1)$
	-2	1	2	$(x_1\text{+}1,y_1\text{+}1)$

$(P_i\text{-}1, P_{i+1}\text{+}1)$	$(P_i, P_{i+1}\text{+}1)$	$(P_i\text{+}1, P_{i+1}\text{+}1)$
$(P_i\text{-}1, P_{i+1})$	(P_i, P_{i+1})	$(P_i\text{+}1, P_{i+1})$
$(P_i\text{-}1, P_{i+1}\text{-}1)$	$(P_i, P_{i+1}\text{-}1)$	$(P_i\text{+}1, P_{i+1}\text{-}1)$

Figure 2: The value of each location in a 3*3 block

8	1	5
4	0	2
7	3	6

Figure 3: The mark of each location in a 3*3 block

their scheme can achieve 1.07 bpp in the embedding capacity. Obviously, the embedding procedure just modifies the original pixel pair to be, at most, plus or minus one, a good visual quality of two stego-images is maintained.

3 Propose Scheme

In this section, we will introduce a novel reversible data hiding scheme to conceal secret data into a grayscale cover image to generate two shadows. It begins with a discussion of the orientation combinations in a 3*3 block, followed by a description of the shadow construction procedure and the data extraction and image recovery procedure of the proposed scheme.

3.1 Orientation Combinations in a 3*3 Block

Suppose we have an cover pixel pair $(P_i,\ P_{i+1})$ and draw a 3*3 block around it. The value of each location is shown in Figure 2. we also mark each location in the block, as shown in Figure 3. It is defined that the smaller mark means a higher priority.

If we embedded some secret data into the pixel pair $(P_i,\ P_{i+1})$ to obtain dual stego-pixel pairs of $(M_i,\ M_{i+1})$ which is denoted as the major one and $(A_i,\ A_{i+1})$ which is denoted as the auxiliary one. Certainly, these stego-pixel pairs are all located within the 3*3 block. In order to achieve reversibility, the orientation combinations of these dual stego-pixel pairs are exploited. To the best of our knowledge, there are a total of 25 combinations which can uniquely determine the center pixel pair $(P_i,\ P_{i+1})$ as shown in Figure 4. Thus, each combination of the dual stego-pixel pairs represents some secret data was embedded in the cover pixel pair. For the convenience, we label these combinations arranging from 0 to 24. The embedding and extracting rules corresponding to these 25 combinations are shown in Table 3. In Table 3, the column labelled as (d_i, d_{i+1}) means the difference between the major and the auxiliary pixel pair which can be acquired by Equation (1). The column labelled as $(P_i,\ P_{i+1})$ is defined as the original pixel pair gained from the major pixel pair in the extracting phase.

$$(d_i,\ d_{i+1}) = (M_i - A_i,\ M_{i+1} - A_{i+1})\ . \tag{1}$$

From Table 3, we can find out that the label of the combination of two dual stego-pixel pairs are ordered by their mark in the 3*3 block. That is, combinations with a smaller major mark is labelled smaller. When two combinations have the same major marks, the smaller auxiliary mark is the smaller label will be. Follow this order, we can create a unique 25 combinations of dual stego-pixel pairs.

According to what's mentioned above, we can embed a base-25 digit into a pixel pair $(P_i,\ P_{i+1})$ to create dual stego-pixel pairs $(M_i,\ M_{i+1})$ and $(A_i,\ A_{i+1})$. Furthermore, the orientation relationship of the dual stego-pixel pairs will depict the embedded digit and the central position where they originated from. The detail of the shadow construction is described in the next section.

3.2 The Shadow Construction Procedure

Assume that a size of R^*C grayscale cover image is divided into a set of pixel pairs $(P_i,\ P_{i+1})$ in raster-scan order, where i$\in$1, 3, $\cdots$, R^*C-1 and a size of n binary stream S is defined as $S = \{s_k\,|k = 1,\ 2, ..., n\}$. We first constructs the table of embedding and extracting rules as mentioned in Section 3.1. Then convert the binary stream into a base-25 digit sequence $S' = \{s'_k\,|k = 1,\ 2, ..., m\}$, where s'_k is arranged from 0 to 24. The converting rules are shown as below:

RULE 1: Get five secret bits $(s_k,\ s_{k+1}, s_{k+2}, s_{k+3}, s_{k+4}\ )$ from binary stream S. Convert them into a decimal value v. If v is less than or equal to 17, then the v is exactly the required digit; Otherwise, read four secret bits $(s_k,\ s_{k+1}, s_{k+2}, s_{k+3}\ )$ from binary stream S. Convert them into the decimal form and increased by "9" to obtain the digit v.

After the sequential of base-25 digits is generated, we will start to process each pixel pair $(P_i,\ P_{i+1})$ in the cover image. If $(P_i,\ P_{i+1})$ belongs to the border, *i.e.*, P_i=0 or P_i=255 or P_{i+1}=0 or P_{i+1}=255, we keep it intact to generate the major pixel pair $(M_i,\ M_{i+1})$ and the auxiliary one $(A_i,\ A_{i+1})$, *i.e.*, M_i=P_i, M_{i+1}=P_{i+1}, A_i=P_i and A_{i+1}=P_{i+1}; otherwise, read a base-25 digit v from S', then rule-v is utilized for creating the two stego-pixel pairs as Equations (2) and (3).

$$(M_i,\ M_{i+1}) \ = \ (M_i,\ M_{i+1})_v\ . \tag{2}$$

$$(A_i,\ A_{i+1}) \ = \ (A_i,\ A_{i+1})_v\ . \tag{3}$$

Where $(M_i,\ M_{i+1})_v$ and $(A_i,\ A_{i+1})_v$ represent the major and auxiliary pixel pairs lying in the embedding rule v in Table 3, respectively.

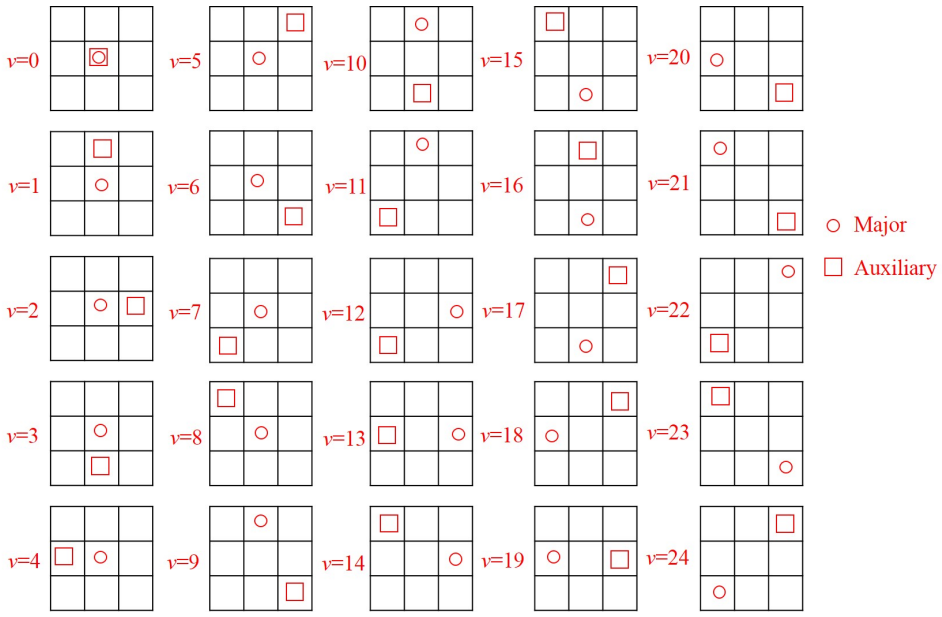

Figure 4: The 25 combinations of dual stego-pixel pairs in a 3*3 block with their labels

Table 3: The embedding and extracting rules of the proposed scheme

v	Secret Bits	(M_i, M_{i+1})	Major Mark	(A_i, A_{i+1})	Auxiliary Mark	(d_i, d_{i+1})	(P_i, P_{i+1})
0	00000	(P_i, P_{i+1})	0	(P_i, P_{i+1})	0	(0,0)	(M_i, M_{i+1})
1	00001			$(P_i, P_{i+1}+1)$	1	(0,1)	
2	00010			(P_i+1, P_{i+1})	2	(1,0)	
3	00011			$(P_i, P_{i+1}-1)$	3	(0,-1)	
4	00100			(P_i-1, P_{i+1})	4	(-1,0)	
5	00101			$(P_i+1, P_{i+1}+1)$	5	(1,1)	
6	00110			$(P_i+1, P_{i+1}-1)$	6	(1,-1)	
7	00111			$(P_i-1, P_{i+1}-1)$	7	(-1,-1)	
8	01000			$(P_i-1, P_{i+1}+1)$	8	(-1,1)	
9	01001	$(P_i, P_{i+1}+1)$	1	$(P_i, P_{i+1}-1)$	3	(0,2)	$(M_i, M_{i+1}-1)$
10	01010			$(P_i+1, P_{i+1}-1)$	6	(-1,2)	
11	01011			$(P_i-1, P_{i+1}-1)$	7	(1,2)	
12	01100	(P_i+1, P_{i+1})	2	(P_i-1, P_{i+1})	4	(2,0)	(M_i-1, M_{i+1})
13	01101			$(P_i-1, P_{i+1}-1)$	7	(2,1)	
14	01110			$(P_i-1, P_{i+1}+1)$	8	(2,-1)	
15	01111	$(P_i, P_{i+1}-1)$	3	$(P_i-1, P_{i+1}+1)$	1	(1,-2)	$(M_i, M_{i+1}+1)$
16	10000			$(P_i+1, P_{i+1}+1)$	5	(-1,-2)	
17	10001			$(P_i, P_{i+1}+1)$	8	(0,-2)	
18	1001	(P_i-1, P_{i+1})	4	(P_i+1, P_{i+1})	2	(-2,0)	(M_i+1, M_{i+1})
19	1010			$(P_i+1, P_{i+1}-1)$	5	(-2,1)	
20	1011			$(P_i+1, P_{i+1}+1)$	6	(-2,-1)	
21	1100	$(P_i+1, P_{i+1}+1)$	5	$(P_i-1, P_{i+1}-1)$	7	(2,2)	$(M_i-1, M_{i+1}-1)$
22	1101	$(P_i+1, P_{i+1}-1)$	6	$(P_i-1, P_{i+1}+1)$	8	(2,-2)	$(M_i-1, M_{i+1}+1)$
23	1110	$(P_i-1, P_{i+1}-1)$	7	$(P_i+1, P_{i+1}+1)$	5	(-2,-2)	$(M_i+1, M_{i+1}+1)$
24	1111	$(P_i-1, P_{i+1}+1)$	8	$(P_i+1, P_{i+1}-1)$	6	(-2,2)	$(M_i+1, M_{i+1}-1)$

After all the pixels are processed, the major stego-image (denoted as M) and auxiliary stego-image (denoted as A) are constructed. For a better understanding of the proposed scheme, an example of the shadow construction procedure is described as follows.

In this example, three cover pixel pairs (0, 2), (5, 6), (8, 8) are used. Suppose the binary stream and the secret stream $(1111\ 00100)_2$ are to be embedded into the pixel pairs. Firstly, we convert binary stream into a base-25 digit sequence of $(24\ 4)_10$ by the converting rule mentioned above. Then, we give more details on how the secret messages are embedded into these pixel pairs to construct two shadows.

1) Since the pixel pair (0, 2) locate in the border, the two stego-pixel pairs are both set to (0, 2) and no secret data is embedded in this case. Thus, the pixel pair of M and A both equal to (0, 2).

2) When embedding the digit 24 into the pixel pair (5, 6). According to Equations (2) and (3), the major and the auxiliary pixel pair are set to $(M_i,\ M_{i+1}) = (M_i,\ M_{i+1})_{24} = (P_i - 1, P_{i+1} + 1) = (4,\ 7)$ and $(A_i,\ A_{i+1}) = (A_i,\ A_{i+1})_{24} = (P_i + 1, P_{i+1} - 1) = (6,\ 5)$. Thus, the pixel pairs of M are (0, 2), (4, 7), while the pixel pairs of A are (0, 2), (6, 5).

3) Follow the similar idea, when embedding the digit 4 into pixel pair (8, 8), According to Equations (2) and (3), the major and the auxiliary pixel pairs are set to $(M_i,\ M_{i+1}) = (M_i,\ M_{i+1})_4 = (P_i, P_{i+1}) = (8,\ 8)$ and $(A_i,\ A_{i+1}) = (A_i,\ A_{i+1})_4 = (P_i - 1, P_{i+1}) = (7,\ 8)$. Finally, the pixel pairs of M are (0, 2), (4, 7), (8, 8), while the pixel pairs of A are (0, 2), (6, 5), (7, 8).

3.3 The Data Extraction and Image Recovery Procedure

In this phase, the receiver can carry out the extraction and restoration by using the corporation of the two shadows. The receiver first generates the identical table of embedding and extracting rules as mentioned in Section 3.1. Then pick up a pixel pair $(M_i,\ M_{i+1})$ from major stego-image M and a pixel pair $(A_i,\ A_{i+1})$ from auxiliary stego-image A at the identical location. The embedded secret bits and the original cover pixel pair can be retrieved by the following way.

1) If M_i=A_i, M_{i+1}=A_{i+1} and M_i=0 or M_i=255, that means the original pixel pair is located at the border, thus P_i=M_i and P_{i+1}=M_{i+1}. Meanwhile, no secret data was embedded in this situation.

2) Calculate d_i and d_{i+1} by Equation (1). The embedding secret base-25 digit v can be determined by $(d_i,\ d_{i+1})$ according to Table 3. Convert v into the binary form to obtain the secret bits, the converting rules is shown as below.

RULE 2: If v is greater than 17, then let v minus 9 and convert the result to a 4-bits binary stream to obtain 4 bits of secret information; otherwise, convert v directly to a 5-bits binary stream to obtain 5 bits of secret information.

Additionally, the cover pixel pair $(P_i,\ P_{i+1})$ is retrieved by

$$(P_i,\ P_{i+1}) = (P_i,\ P_{i+1})_v. \tag{4}$$

Where $(P_i,\ P_{i+1})_v$ represents the cover pixel pair lying in the embedding rule v in Table 3.

After all pixel pairs of two stego-images have been processed, the secret binary stream S and the original cover image can be can be retrieved exactly. Continue the example described in Section 3.2, we will illustrate how to extract the secret data and retrieve the cover image by using the pixel pairs of M(0, 2), (4, 7), (8, 8) and A(0, 2), (6, 5), (7, 8).

1) Obviously, for the identical pixel pair (0, 2) from M and A, the cover pixel pair is located at the border and equals to (0, 2). No secret data was concealed in this situation.

2) Pick up the next pixel pairs (4, 7) and (6, 5) from M and A, respectively. According to Equation (1), the $(d_i,\ d_{i+1})$ can be calculated by $(d_i,\ d_{i+1}) = (4 - 6,\ 7 - 5) = (-2,\ 2)$. Examine $(d_i,\ d_{i+1})$ in Table 3 which can determine that digit 24 is embedded in this situation. According to the *RULE* 2, digit 24 is greater than 17, thus convert (24-9) =15 into a 4-bit binary stream "1111" which is exactly the secret data. Meanwhile, the cover pixel can be retrieved by Equation (4) which is $(P_i,\ P_{i+1}) = (P_i,\ P_{i+1})_{24} = (M_i + 1,\ M_{i+1} - 1) = (4 + 1,\ 7 - 1) = (5,\ 6)$. Thus, the binary secret bit stream S becomes $(1111)_2$ and the cover pixel pairs are (0, 2), (5, 6).

3) Continue to take pixel pairs (8, 8) and (7, 8) into consideration. Calculate the $(d_i,\ d_{i+1})$ by Equation (1) which is $(d_i,\ d_{i+1}) = (8 - 7,\ 8 - 8) = (1,\ 0)$. According to Table 3, we can determine that digit 4 is embedded by the value of $(d_i,\ d_{i+1})$. Secret data "00100" is retrieved by digit 4 according to *RULE* 2. Similarly, the cover pixel can be retrieved by Equation (4) that $(P_i,\ P_{i+1}) = (P_i,\ P_{i+1})_4 = (M_i,\ M_{i+1}) = (8,\ 8)$. Finally, the binary secret bit stream S becomes $(1111\ 00110)_2$ and the cover pixel pairs are (0, 2), (5, 6), (8, 8). The secret data and cover pixel pairs are all retrieved without any error.

4 Experimental Results

The simulation is implemented by Matlab R2012b software on the Intel Core (TM) i5-4210U at 1.70 GHz, 8 GB main memory. Additionally, the operating system is

Windows 7. The binary secret bit stream S is randomly generated using a secret key, *i.e.*, $key1$=2018.

Two conventional measurements are used to evaluate the performance of a data hiding scheme, *i.e.*, the embedding capacity and visual quality of the generated stego-image. In our experiment, the embedding ratio ξ is employed to estimate the embedding capacity (bpp) of a data hiding scheme to carry the pure secret data which is defined as

$$\xi = NUM/\left(2 \times R \times C\right) \ . \tag{5}$$

Where NUM represents the total number of secret bits which are embedded into two stego-images. Additionally, parameters R and C refer to the height and width of the cover image. ξ is divided by 2 because we finally generated two stego-images. Furthermore, the PSNR is used to evaluate the image quality (dB) which is defined as

$$PSNR = 10\log_{10}\left(\frac{255^2 \times R \times C}{\sum_{i=1}^{R}\sum_{j=1}^{C}\left(O_{ij} - SH_{ij}\right)^2}\right) \tag{6}$$

Where O_{ij} and SH_{ij} are referred to the pixels located at the i-th row and the j-th column of cover image O and stego-image SH, respectively.

4.1 Security Enhancement

To enhance the security of the proposed scheme, we generate a random binary bit string which is denoted as $F = \{f_1 f_2 ... f_n,\ f_i = \{0,1\},\ i \in [1,n]\}$, where n represents the number of pixel pairs in original image. Similarly, the binary stream is randomly generated by a secret key, *i.e.*, $key2$=2018. The random bit in private key F is utilized to determine which pixel pair to play what kind of role, *i.e.*, which one is the major and which is the auxiliary. In this paper, we set up that f_i=1 indicates the i-th pixel pair of first stego-image which is considered to be the major pixel pair and the same sequential pixel pair of the second stego-image served as auxiliary. The setting is exactly the opposite to the situation of f_i=0. Figure 5 shows the principle of the enhancement of one cover pixel pair.

4.2 Comparison with Previous Schemes

In the simulation analysis, we employed eight images with size of 512*512 (as shown in Figure 6) to show the embedding capacity and the visual quality of each stego-image of the proposed scheme compared to some previous methods.

To verify the efficiency of the proposed scheme after the security enhancement, comparative results with some state-of-the-art methods in [17–19] measured by and PSNR are given in Table 4 and Table 5, respectively. Notices that, the methods in [17, 18] are using the security enhancement while the scheme in [19] is not.

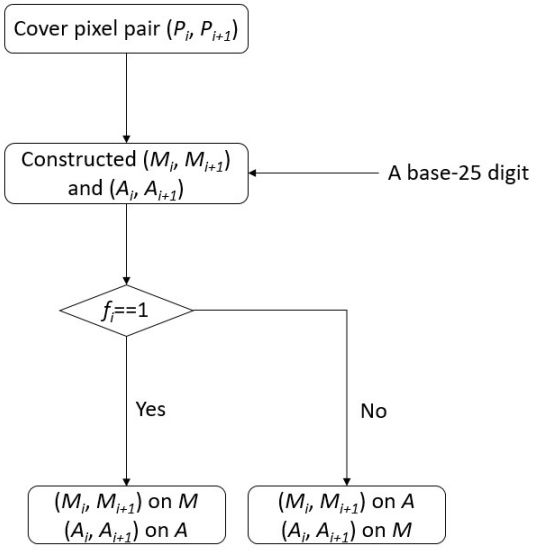

Figure 5: Security enhancement for one cover pixel pair

Figure 6: Eight 512*512 grayscale images

Table 4: Comparative embedding ratio of different schemes

Images	[18]	[17]	[19]	Proposed scheme
Baboon	0.74	1.07	1	1.14
Barbara	0.74	1.07	1	1.14
Lena	0.74	1.07	1	1.14
Pepper	0.74	1.07	1	1.14
Elaine	0.74	1.07	0.99	1.14
Goldhill	0.74	1.07	1	1.14
Airplane	0.74	1.07	1	1.14
Wine	0.74	1.07	1	1.14
Average	**0.74**	**1.07**	**1**	**1.14**

Table 5: Comparative image qualities of the shadows of different schemes

Images	[18]		[17]		[19]		Proposed scheme	
	M	*A*	*M*	*A*	*M*	*A*	*M*	*A*
Baboon	52.47	52.47	49.38	49.38	51.72	45.71	49.91	49.92
Barbara	52.47	52.48	49.38	49.38	51.73	45.70	49.91	49.92
Lena	52.47	52.48	49.38	49.38	51.69	45.70	49.91	49.92
Peppers	52.47	52.48	49.38	49.38	51.73	45.70	49.91	49.92
Elaine	52.47	52.48	49.38	49.38	51.84	45.66	49.91	49.92
Goldhill	52.47	52.48	49.38	49.38	51.72	45.71	49.91	49.92
Airplane	52.47	52.48	49.38	49.38	51.68	45.73	49.91	49.92
Wine	52.47	52.47	49.38	49.38	51.67	45.72	49.91	49.92
Average	**52.47**	**52.48**	**49.38**	**49.38**	**51.72**	**45.70**	**49.91**	**49.92**

From Table 4, it is shown that the proposed scheme acquires the best embedding ratio ξ of 1.14 bpp. The gains of the average ξ of the proposed scheme are 0.4 bpp and 0.07 bpp, and 0.14 bpp compared to these three comparative schemes in [17–19], respectively.

In Table 5, we focused on the average level. Though the scheme in [18] gains the best visual quality of up to 52.48 dB, his embedding ratio ξ is smaller than the proposed scheme of 0.4 bpp. The results also show that the proposed scheme achieves a PSNR of 0.55 dB higher than [17]. While comparing to [19], the proposed scheme has 1.81 dB lower in the main image, but 4.22 dB higher for the auxiliary one.

4.3 PVD Histogram Analysis

The robustness of the proposed scheme can be measured by PVD histogram. It creates a histogram through the different value of two consecutive pixels. The closer the shadow PVD histogram is to the cover PVD histogram, the better the scheme is. Figure 7 shows the PVD histograms of the four cover images (a)-(d) and their shadows. Obviously, the shape of the cover PVD histogram is well preserved on two shadows.

5 Conclusions

This work exploits the combinations of pixel pair orientations in two stego-images. There are at most 25 combinations which can uniquely determine where the two stego-pixel pair are originated from. While labelling these combinations from 0 to 24 by a particular order, each combination can represent the embedding of a base-25 digit and no overhead message is needed for secret data extraction and original image recovery. The stego-pixel pairs are only altering the cover value by at most plus one or minus one, so the generated stego-images can achieve high image quality. Experimental results indicate that a high embedding capacity of 1.14 bpp can be achieved in the proposed scheme and the average image quality of 49.92 dB of the two stego-images is gained. Moreover, the proposed scheme can resist the static attacks on PVD histogram.

Acknowledgments

This study was supported by Fujian Province Education and Science Foundation of young teachers (JAT170619). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

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

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of American Federation of Information Processing Societies National Computer Conference*, pp. 313–317, Nov. 1979.

[3] C. K. Chan and L. M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[4] C. C. Chang, Y. C. Chou and T. D. Kieu, "An information hiding scheme using sudoku," in *Proceedings of Third International Conference on Innovative Computing, Information and Control*, June 2008.

[5] C. C. Chang, Y. J. Liu and T. S. Nguyen, "A novel turtle shell based scheme for data hiding," in *Proceedings of Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 89–93, Aug. 2014.

[6] C. C. Chang, Y. C. Chou and T. D. Kieu, "Information hiding in dual images with reversibility," in *Proceedings of the Third International Conference on Multimedia and Ubiquitous Engineering*, pp. 145–152, June 2009.

[7] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

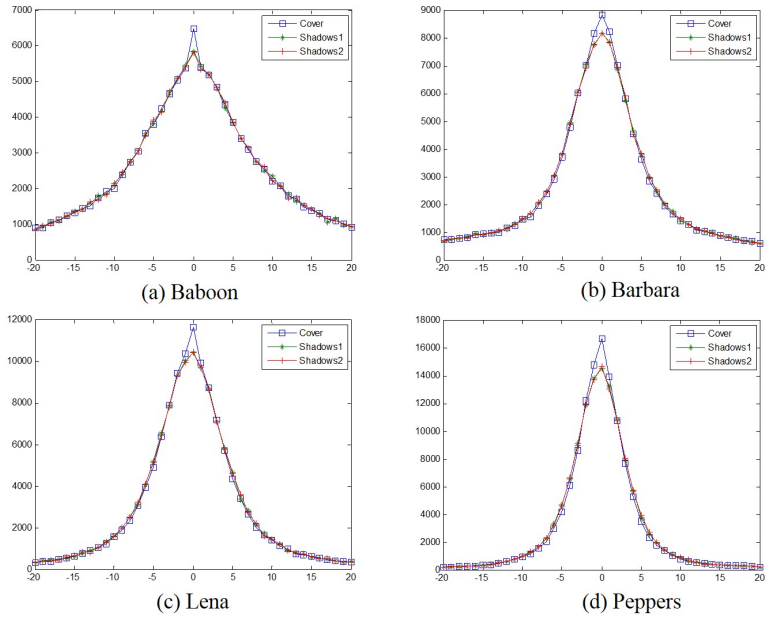

Figure 7: Four PVD histograms of the cover images and their shadows

[8] C. C. Chang, T. D. Kieu and Y.C. Chou, "Reversible data hiding scheme using two steganographic images," in *Proceedings of IEEE Region 10 International Conference (TENCON'07)*, pp. 1–4, Nov. 2007.

[9] C. C. Chang, T. C. Lu, G. Horng, Y. H. Huang and Y. M. Hsu, "A high payload data embedding scheme using dual stego-images with reversibility," in *Proceedings of the Third International Conference on Information, Communications and Signal Processing*, pp. 1–5, Dec. 2013.

[10] I. C. Chang, Y. C. Hu, W. L. Chen and C. C. Lo, "High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding," *Signal Processing*, vol. 108, pp. 376–388, 2015.

[11] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 20–31, 2018.

[12] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.

[13] L. C. Huang, L. Y. Tseng, M. S. Hwang, "The study on data hiding in medical images", *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[14] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.

[15] H. J. Kim, C. Kim, Y. Choi, S. Wang and X. Zhang, "Improved modification direction schemes," *Computer and Mathematics with Applications*, vol. 60, no. 2, pp. 319–325, 2010.

[16] C. F. Lee, J. J. Li, Y. H. Wu and C. C. Chang, "Generalized pvo-k embedding technique for reversible data hiding," *International Journal of Network Security*, vol. 20, no. 1, pp. 65–77, 2018.

[17] C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," *Telecommunication Systems*, vol. 52, no. 4, pp. 2237–2247, 2011.

[18] C. F. Lee, K. H. Wang, C. C. Chang and Y. L. Huang, "A reversible data hiding scheme based on dual steganographic images," in *Proceedings of the Third International Conference on Ubiquitous Information Management and Communication*, pp. 228–237, Jan. 2009.

[19] Y. Liu and C. C. Chang, "A turtle shell-based visual secret sharing scheme with reversibility and authentication," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25295–25310, 2018.

[20] Y. J. Liu, C. C. Chang and T. S. Nguyen, "High capacity turtle shell-based data hiding," *IET Image Processing*, vol. 10, no. 2, pp. 130–137, 2016.

[21] J. Mielikainen, "Lsb matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 6, pp. 1129–1143, 2009.

[22] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[23] C. Qin, C. C. Chang and T. J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images," *Multimedia Tools and Applications*, vol. 74, no. 15, pp. 5861–5872, 2015.

[24] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.
[25] J. J. Shen, Y. L. Wang and M. S. Hwang, "An improved dual image-based reversible hiding technique using lsb matching," *International Journal of Network Security*, vol. 20, no. 4, pp. 801–804, 2018.
[26] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.
[27] P. Y. Tsai, Y. C. Hu and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129–1143, 2009.
[28] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2013.
[29] X. P. Zhang and S. Z. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781–783, 2006.

Biography

Xiaofeng Chen. Received the B.S degree from Fujian Normal University in 1999 and the M.S degree from Fuzhou University, Fujian, China, in 2008. He is currently a lecturer with the School of Electronic Information Science, Fujian Jiangxia University. His research interests include information hiding, privacy protection and quantum cryptography.

Wenlong Guo. Received the B.S degree from Southwest University for Nationalities, Sichuan, China, in 2002 and the M.S degree from Fuzhou University, Fujian, China, in 2011. He is currently an associate professor with the School of Electronic Information Science, Fujian Jiangxia University. His research interests include information hiding , cryptography and data mining.