A Novel Data Embedding Method Using Adaptive Pixel Pair Matching

Wien Hong and Tung-Shou Chen

***Abstract*—This paper proposes a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighborhood sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads. Experimental results reveal that the proposed method not only provides better performance than those of OPAP and DE, but also is secure under the detection of some well-known steganalysis techniques.**

***Index Terms*—Adaptive pixel pair matching (APPM), diamond encoding (DE), exploiting modification direction (EMD), least significant bit (LSB), optimal pixel adjustment process (OPAP), pixel pair matching (PPM).**

I. Introduction

DATA hiding is a technique that conceals data into a carrier for conveying secret messages confidentially [1], [2]. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are termed as cover images and images with data embedded are termed as stego images. After embedding, pixels of cover images will be modified and distortion occurs. The distortion caused by data embedding is called the embedding distortion [3]. A good data-hiding method should be capable of evading visual and statistical detection [4] while providing an adjustable payload [5].

Manuscript received February 28, 2011; accepted April 16, 2011. Date of publication May 16, 2011; date of current version January 13, 2012. This work was supported by the National Science Council of the Republic of China under Grant NSC100-2622-E-412-003-CC3 and Grant NSC 100-2221-E-412-003. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wenjun Zeng.

W. Hong is with the Department of Information Management, Yu Da University, Tanwen Village, Chaochiao Township, Miaoli County 361, Taiwan (e-mail: wienhong@ydu.edu.tw).

T.-S. Chen is with the Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung 404, Taiwan (e-mail: tschen@ntit.edu.tw).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2011.2155062

The least significant bit substitution method, referred to as LSB in this paper, is a well-known data-hiding method. This method is easy to implement with low CPU cost, and has become one of the popular embedding techniques. However, in LSB embedding, the pixels with even values will be increased by one or kept unmodified. The pixels with odd values will be decreased by one or kept unmodified. Therefore, the imbalanced embedding distortion emerges and is vulnerable to steganalysis [6], [7]. In 2004, Chan *et al.* [8] proposed a simple and efficient optimal pixel adjustment process (OPAP) method to reduce the distortion caused by LSB replacement. In their method, if message bits are embedded into the right-most r LSBs of an m-bit pixel, other $m-r$ bits are adjusted by a simple evaluation. Namely, if the adjusted result offers a smaller distortion, these $m-r$ bits are either replaced by the adjusted result or otherwise kept unmodified.

The LSB and OPAP methods employ one pixel as an embedding unit, and conceal data into the right-most r LSBs. Another group of data-hiding methods employs two pixels as an embedding unit to conceal a message digit s_B in a B-ary notational system. We term these data-hiding methods as pixel pair matching (PPM). In 2006, Mielikainen [9] proposed an LSB matching method based on PPM. He used two pixels as an embedding unit. The LSB of the first pixel is used for carrying one message bit, while a binary function is employed to carry another bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance a pixel value has to be changed by one yet another 1/4 chance no pixel has to be modified. Accordingly, the MSE is $(3/4) \times (1^2/2) = 0.375$ when payload is 1 bpp [9]. In contrast, the MSE obtained by LSB is 0.5. In the same year, Zhang and Wang [10] proposed an exploiting modification direction (EMD) method. EMD improves Mielikainen's method in which only one pixel in a pixel pair is changed one gray-scale unit at most and a message digit in a 5-ary notational system can be embedded. Therefore, the payload is $(1/2)\log_2 5 = 1.161$ bpp. LSB matching and EMD methods greatly improve the traditional LSB method in which a better stego image quality can be achieved under the same payload. However, the maximum payloads of LSB matching and EMD are only 1 and 1.161 bpp, respectively. Hence, these two methods are not suitable for applications requiring high payload.

The embedding method of LSB matching and EMD offers no mechanism to increase the payload. In 2008, Hong [11] presented a data-hiding method based on Sudoku solutions to achieve a maximum payload of $(1/2)\log_2 9$ bpp. In 2009, Chao *et al.* [12] proposed a diamond encoding (DE) method to enhance the payload of EMD further. DE employs an extraction function to generate diamond characteristic values (DCV), and

embedding is done by modifying the pixel pairs in the cover image according to their DCV's neighborhood set and the given message digit. Chao used an embedding parameter k to control the payload, in which a digit in a B-ary notational system can be concealed into two pixels, where $B = 2k^2 + 2k + 1$. If $k = 1$, $B = 5$, i.e., digits in a 5-ary notational system are concealed, the resultant payload is equivalent to EMD. If $k = 2$, $B = 13$; if $k = 3$, $B = 25$. Note that B is significantly increased as k is only increased by one. Instead of enhancing the payload of EMD, Wang *et al.* [13] in 2010 proposed a novel section-wise exploring modification direction method to enhance the image quality of EMD. Their method segments the cover image into pixel sections, and each section is partitioned into the selective and descriptive groups. The EMD embedding procedure is then performed on each group by referencing a predefined selector and descriptor table. This method combines different pixel groups of the cover image to represent more embedding directions with less pixel changes than that of the EMD method. By selecting the appropriate combination of pixel groups, the embedding efficiency and the visual quality of the stego image is enhanced.

Another group of rather practical data-hiding methods considers security as a guiding principle for developing a less detectable embedding scheme. These methods may either be implemented by avoiding embedding the message into the conspicuous part of the cover image, or by improving the embedding efficiency, that is, embed more messages per modification into the cover [14]. The former can be achieved, for example, using "the selection channel" such as the wet paper code proposed by Fridrich *et al.* [15]. The latter can be done by encoding the message optimally with the smallest embedding impact using the near-optimal embedding schemes [4], [16], [17]. In these methods, the data bits were not conveyed by individual pixels but by groups of pixels and their positions.

This paper proposes a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency. The image quality obtained by the proposed method not only performs better than those obtained by OPAP and DE, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.

The rest of this paper is organized as follows. Section II is a brief review of OPAP and DE. The proposed method is given in Section III. Experimental results are given in Section IV, and the steganalysis of the proposed method is presented in Section V. Section VI includes the conclusions and remarks.

II. Related Works

OPAP effectively reduces the image distortion compared with the traditional LSB method. DE enhances the payload of EMD by embedding digits in a B-ary notational system. These two methods offer a high payload while preserving an acceptable stego image quality. In this section, OPAP and DE will be briefly reviewed.

A. Optimal Pixel Adjustment Process (OPAP)

The OPAP method proposed by Chan *et al.* in 2004 greatly improved the image distortion problem resulting from LSB replacement. The OPAP method is described as follows [8], [18]. Suppose a pixel value is v, the value of the right-most r LSBs of v is $v^{(r)}$. Let v' be the pixel value after embedding r message bits using the LSB replacement method and s be the decimal value of these r message bits. OPAP employs the following equation to adjust v' so that the embedding distortion can be minimized

$$v'' = \begin{cases} v' + 2^r, & v^{(r)} - s > 2^{r-1} \text{ and } v' + 2^r \le 255 \\ v' - 2^r, & v^{(r)} - s < -2^{r-1} \text{ and } v' - 2^r \ge 0 \\ v', & \text{otherwise} \end{cases}$$

where v'' denotes the result obtained by OPAP embedding. Note that v'' and v' have the same right-most r LSBs and thus, the embedded data can be extracted directly from the right-most r LSBs. Here is a simple example. Suppose a pixel value $v = 160 = 10100000_2$ and the bits to be embedded are 101_2. In this case, $r = 3$ and $s = 5$. After s is embedded, we obtained $v' = 165$. Because $v^{(3)} = 000_2 = 0$ and $v^{(3)} - s = 0 - 5 < -2^{3-1}$, we obtained $v'' = v' - 2^3 = 165 - 8 = 157 = 10011101_2$. Thus, after embedding 101_2, the pixel value 160 is changed to 157. To extract the embedded data, we simply extract the right-most three LSBs of 157.

B. Diamond Encoding

In 2009, Chao *et al.* proposed a DE method based on PPM. This method conceals a secret digit in a B-ary notational system into two pixels, where $B = 2k^2+2k+1$, $k \ge 1$. The payload of DE is $(1/2)\log_2(2k^2 + 2k + 1)$ bpp. Note that when $k = 1$, DE is equivalent to EMD in which both methods conceal digits in a 5-ary notational system. The DE method is briefly described as follows.

Let the size of m bits cover image be $M \times M$, message digits be S_B, where the subscript B represents S_B is in a B-ary notational system. First, the smallest integer k is determined to satisfy the following equation:

$$\left\lfloor \frac{M \times M}{2} \right\rfloor \ge |S_B|$$

where $|S_B|$ denotes the number of message digits in a B-ary notational system. To conceal a message digit s_B into pixel pair (x, y), the neighborhood set $\Phi(x, y)$ is determined by

$$\Phi(x, y) = \{(a, b) \big| |a - x| + |b - y| \le k\}$$

where $\Phi(x, y)$ represents the set of the coordinates (a, b)'s whose absolute distance to the coordinate (x, y) is smaller or equal to k. A diamond function f is then employed to calculate the DCV of (x, y), where $f(x, y) = ((2k + 1)x + y) \bmod B$. After that, the coordinates belong to the set $\Phi(x, y)$ are searched and DE finds a coordinate (x', y') satisfying $f(x', y') = s_B$, and then (x, y) is replaced by (x', y'). Repeat these procedures until all the message digits are embedded. In the extraction

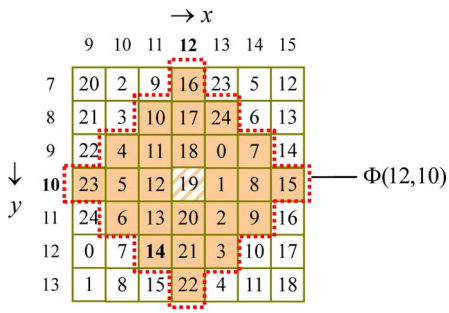

Fig. 1. Neighborhood set $\Phi(12, 10)$ for $k = 3$.

phase, pixels are scanned using the same order as in the embedding phased. The DCV value of a pixel pair (x', y') is then extracted as a message digit.

Here is a simple example. Let $k = 3$ and $(x, y) = (12, 10)$, then $B = 2 \times 3^2 + 2 \times 3 + 1 = 25$. The neighborhood set $\Phi(12, 10)$ and its corresponding DCV values are shown in Fig. 1. If a digit in a 25-ary notational system 14_{25} needs to be embedded, then in the region defined by $\Phi(12, 10)$, we find the DCV value of $(x', y') = (11, 12) = 14$. Therefore, we simply replace (12,10) by (11,12) and the digit 14_{25} is embedded. To extract the embedded digits, we calculate $f(x', y') = f(11, 12) = (7 \times 11 + 12) \bmod 25 = 14$; the calculation result 14 is then the embedded digit.

III. Adaptive Pixel Pair Matching (APPM)

The basic idea of the PPM-based data-hiding method is to use pixel pair (x, y) as the coordinate, and searching a coordinate (x', y') within a predefined neighborhood set $\Phi(x, y)$ such that $f(x', y') = s_B$, where f is the extraction function and s_B is the message digit in a B-ary notational system to be concealed. Data embedding is done by replacing (x, y) with (x', y').

For a PPM-based method, suppose a digit s_B is to be concealed. The range of s_B is between 0 and $B - 1$, and a coordinate $(x', y') \in \Phi(x, y)$ has to be found such that $f(x', y') = s_B$. Therefore, the range of $f(x, y)$ must be integers between 0 and $B - 1$, and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in $\Phi(x, y)$ should be as small as possible. The best PPM method shall satisfy the following three requirements: 1) There are exactly B coordinates in $\Phi(x, y)$. 2) The values of extraction function in these coordinates are mutually exclusive. 3) The design of $\Phi(x, y)$ and $f(x, y)$ should be capable of embedding digits in any notational system so that the best B can be selected to achieve lower embedding distortion.

DE is a data-hiding method based on PPM. DE greatly enhances the payload of EMD while preserving acceptable stego image quality. However, there are several problems. First, the payload of DE is determined by the selected notational system, which is restricted by the parameter k; therefore, the notational system cannot be arbitrarily selected. For example, when k is 1, 2, and 3, then digits in a 5-ary, 13-ary, and 25-ary notational system are used to embed data, respectively. However, embedding digits in a 4-ary (i.e., 1 bit per pixel) or 16-ary (i.e., 2 bits per pixel) notational system are not supported in DE. Second, $\Phi(x, y)$ in DE is defined by a diamond shape, which may lead to some unnecessary distortion when $k > 2$. In fact, there exists a better $\Phi(x, y)$ other than diamond shape resulting in a smaller embedding distortion. In Section III-A, we redefine $\Phi(x, y)$ as well as $f(x, y)$ and then propose a new embedding method based on PPM. The proposed method not only allows concealing digits in any notational system, but also provides the same or even smaller embedding distortion than DE for various payloads.

A. Extraction Function and Neighborhood Set

The definitions of $\Phi(x, y)$ and $f(x, y)$ significantly affect the stego image quality. The designs of $\Phi(x, y)$ and $f(x, y)$ have to fulfill the requirements: all values of $f(x, y)$ in $\Phi(x, y)$ have to be mutually exclusive, and the summation of the squared distances between all coordinates in $\Phi(x, y)$ and (x, y) has to be the smallest. This is because, during embedding, (x, y) is replaced by one of the coordinates in $\Phi(x, y)$. Suppose there are B coordinates in $\phi(x, y)$, i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (x, y) by one of the coordinates in $\Phi(x, y)$ is equivalent. The averaged MSE can be obtained by averaging the summation of the squared distance between (x, y) and other coordinates in $\Phi(x, y)$. Thus, given a $\Phi(x, y)$, the expected MSE after embedding can be calculated by

$$\mathrm{MSE}_{\Phi(x,y)} = \frac{1}{2B} \sum_{i=0}^{B-1} \left((x_i - x)^2 + (y_i - y)^2 \right).$$

Here we will propose an adaptive pixel pair matching (APPM) data-hiding method to explore better $f(x, y)$ and $\Phi(x, y)$ so that $\mathrm{MSE}_{\Phi(x,y)}$ is minimized. Data is then embedded by using PPM based on these $f(x, y)$ and $\Phi(x, y)$. Let

$$f(x, y) = (x + c_B \times y) \bmod B.$$

The solution of $\Phi(x, y)$ and $f(x, y)$ is indeed a discrete optimization problem

$$\begin{aligned} \text{Minimize:} \quad & \sum_{i=0}^{B-1} (x_i - x)^2 + (y_i - y)^2 \\ \text{Subject to:} \quad & f(x_i, y_i) \in \{0, 1, \ldots, B-1\} \\ & f(x_i, y_i) \neq f(x_j, y_j), \quad \text{if } i \neq j \\ & \text{for } 0 \leq i, j \leq B-1. \end{aligned} \tag{1}$$

Given an integer B and an integer pair (x, y), (1) can be solved to obtain a constant c_B and B pairs of (x_i, y_i). These B pairs of (x_i, y_i) are denoted by $\Phi_B(x, y)$. Note that $\Phi_B(x, y)$ represents a neighborhood set of (x, y). Table I lists the constant c_B satisfying (1) for the payloads under 3 bpp. Note that, for a given B, it is possible to have more than one c_B and $\Phi_B(x, y)$ satisfying (1). Table I only lists the smallest c_B.

Fig. 2 shows some representative $\Phi_B(x, y)$ and their corresponding c_B satisfying (1), where the center of $\Phi_B(x, y)$ is shaded with lines. Note that, in DE, setting $k = 3$ and $k = 4$, respectively, embeds digits in the 25-ary and 41-ary notational systems. We also depict the $\Phi(x, y)$ of DE when setting $k = 3$ and $k = 4$ in Fig. 2. Note that the four corners of the diamond

TABLE I
LIST OF THE CONSTANT c_B FOR $2 \le B \le 64$

c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	c_{17}	c_{18}
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6	4	4
c_{19}	c_{20}	c_{21}	c_{22}	c_{23}	c_{24}	c_{25}	c_{26}	c_{27}	c_{28}	c_{29}	c_{30}	c_{31}	c_{32}	c_{33}	c_{34}	c_{35}
4	8	4	5	5	5	10	5	5	5	12	12	7	6	6	10	
c_{36}	c_{37}	c_{38}	c_{39}	c_{40}	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}	c_{46}	c_{47}	c_{48}	c_{49}	c_{50}	c_{51}	c_{52}
15	6	16	7	7	6	12	12	8	7	7	7	7	14	14	9	22
c_{53}	c_{54}	c_{55}	c_{56}	c_{57}	c_{58}	c_{59}	c_{60}	c_{61}	c_{62}	c_{63}	c_{64}					
8	12	21	16	24	22	9	8	8	8	14	14					

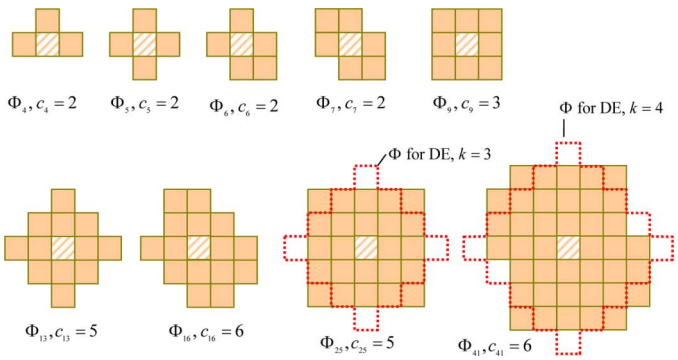

Fig. 2. Neighborhood set (shaded region) for APPM.

shape may cause larger MSE but ours selects a more compact region for embedding, and thus smaller distortion can be achieved.

B. Embedding Procedure

Suppose the cover image is of size $M \times M$, S is the message bits to be concealed and the size of S is $|S|$. First we calculate the minimum B such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input: Cover image I of size $M \times M$, secret bit stream S, and key K_r.

Output: Stego image I', c_B, $\Phi_B(x, y)$, and K_r.

1. Find the minimum B satisfying $\lfloor M \times M/2 \rfloor \ge |S_B|$, and convert S into a list of digits with a B-ary notational system S_B.
2. Solve the discrete optimization problem to find c_B and $\Phi_B(x, y)$.
3. In the region defined by $\Phi_B(0, 0)$, record the coordinate $(\hat{x}_i, \hat{y}_i)$ such that $f(\hat{x}_i, \hat{y}_i) = i, 0 \le i \le B - 1$.
4. Construct a nonrepeat random embedding sequence Q using a key K_r.
5. To embed a message digit s_B, two pixels (x, y) in the cover image are selected according to the embedding sequence Q, and calculate the modulus distance [14] $d = (s_B - f(x, y)) \bmod B$ between s_B and $f(x, y)$, then replace (x, y) with $(x + \hat{x}_d, y + \hat{y}_d)$.
6. Repeat Step 5 until all the message digits are embedded.

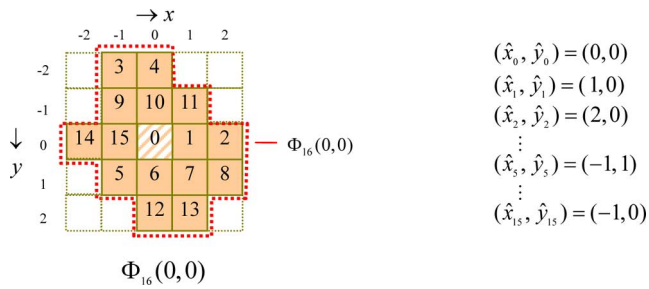

Fig. 3. Neighborhood set $\Phi_{16}(0, 0)$ and $(\hat{x}_i, \hat{y}_i)$, where $0 \le i \le B - 1$.

In real applications, we can solve all c_B and $\Phi_B(x, y)$ at once. With the knowledge of c_B and $\Phi_B(x, y)$, there is no need to perform Step 2 in the embedding phase.

Let $x' = x + \hat{x}_d$ and $y' = y + \hat{y}_d$. If an overflow or underflow problem occurs, that is, $(x', y') < 0$ or $(x', y') > 255$, then in the neighborhood of (x, y) find a nearest (x'', y'') such that $f(x'', y'') = s_B$. This can be done by solving the optimization problem

$$\begin{aligned} &\text{Minimize} && (x - x'')^2 + (y - y'')^2 \\ &\text{Subject to} && f(x'', y'') = s_B, \quad 0 \le x'', y'' \le 255. \end{aligned}$$

We use a simple example to illustrate the embedding procedure. Suppose a cover image of size 512×512 with embedding requirement of 520 000 bits. The minimum B satisfying $(512 \times 512 \times \log_2 B)/2 \ge 520\,000$ is 16; therefore, we choose the 16-ary notational system as the embedding base. After the notational system is known, $c_{16} = 6$ and $\Phi_{16}(x, y)$ can be obtained by solving (1). The 16 $(\hat{x}_i, \hat{y}_i)$'s in $\Phi_{16}(0, 0)$ such that $f(\hat{x}_i, \hat{y}_i) = i$, $0 \le i \le 15$ are recorded. The neighborhood set $\Phi_{16}(0, 0)$ and $(\hat{x}_i, \hat{y}_i)$, where $0 \le i \le 15$, are shown in Fig. 3. Suppose a pixel pair (10,11) that is to be concealed a digit 1_{16} in a 16-ary notational system. The modulus distance between 1_{16} and $f(10, 11)$ is $d = (1 - 12) \bmod 16 = 5$ and $(\hat{x}_5, \hat{y}_5) = (-1, 1)$; therefore, we replace (10, 11) by $(10 - 1, 11 + 1) = (9, 12)$.

C. Extraction Procedure

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.

Input: Stego image I', c_B, $\Phi(x, y)$, and K_r.

Output: Secret bit stream S.

1. Construct the embedding sequence Q using the key K_r.
2. Select two pixels (x', y') according to the embedding sequence Q.
3. Calculate $f(x', y')$, the result is the embedded digit.
4. Repeat Steps 2 and 3 until all the message digits are extracted.
5. Finally, the message bits S can be obtained by converting the extracted message digits into a binary bit stream.

Continue from the previous example. Let the scanned pixel pair be $(x', y') = (9, 12)$. The embedded digit in a 16-ary notational system can be extracted by calculating $f(9, 12) = (9 + 6 \times 12) \bmod 16 = 1_{16}$.

IV. Quality Analysis and Experimental Results

Image distortion occurs when data are embedded because pixel values are modified. We use MSE to measure the image quality

$$\mathrm{MSE} = \frac{1}{M \times M} \sum_{i=0}^{M} \sum_{j=0}^{M} \left(p_{i,j} - p'_{i,j}\right)^2$$

where $M \times M$ denotes the image size, $p_{i,j}$ and $p'_{i,j}$ denote the pixel values of the original image and the stego image, respectively. MSE represents the mean square error between the cover image and stego image. A smaller MSE indicates that the stego image has better image quality.

A. Analysis of Theoretical MSE

In this section, we analyze the averaged MSE of LSB, OPAP, DE, and APPM so that the stego image quality obtained from each method can be theoretically measured. When data are embedded using r LSBs of each pixel, each bit valued 0 or 1 has equal probability. The squared error caused by embedding a bit in the ith LSB is $(1/2)(2^{i-1})^2$; therefore, the averaged MSE of embedding r LSBs is given by

$$\mathrm{MSE}_{\mathrm{LSB}} = \frac{1}{2} \sum_{i=1}^{r} (2^{i-1})^2 = \frac{1}{6}(4^r - 1). \tag{2}$$

Now we analyze the averaged MSE of OPAP when r message bits are embedded in each pixel. Let the original pixel value be v and the stego pixel value be v''. The probability of $|v - v''| = 0$ or $|v - v''| = 2^{r-1}$ is $1/2^r$; the probability of $|v - v''|$ to be within the range $[1, 2^{r-1} - 1]$ is $1/2^r$. Therefore, the averaged MSE caused by embedding r bits is

$$\mathrm{MSE}_{\mathrm{OPAP}} = \frac{1}{2^r}(2^{r-1})^2 + \frac{1}{2^{r-1}} \sum_{i=1}^{2^{r-1}-1} i^2 = \frac{1}{12}(4^r + 2). \tag{3}$$

Note that when $r = 1$, OPAP and LSB have the same MSE. In other words, OPAP cannot reduce the distortion caused by LSB embedding at 1 bpp.

For the DE method, assume that the probability of selecting a coordinate (x_i, y_i) in the diamond shape $\Phi(x, y)$ to replace a pixel pair (x, y) is the same. Therefore, the averaged MSE caused by embedding digits in a B-ary notational system is

$$\begin{aligned}\mathrm{MSE}_{\mathrm{DE}} &= \frac{1}{2B} \sum_{i=0}^{B-1} \left((x_i - x)^2 + (y_i - y)^2\right) \\ &= \frac{1}{2B} \left(\sum_{y=0}^{k} \sum_{x=y-k}^{k-y} (x^2 + y^2) + \sum_{y=1}^{k} \sum_{x=y-k}^{k-y} (x^2 + y^2) \right) \\ &= \frac{k(k+1)(k^2+k+1)}{3 + 6k(k+1)}\end{aligned} \tag{4}$$

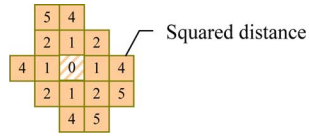

Fig. 4. Calculation of theoretical averaged MSE for APPM with $B = 16$.

TABLE II
MSE Comparison of the Proposed Method With LSB and OPAP

Payload (bpp)	LSB	OPAP	APPM	MSE improvement over OPAP
1	0.500	0.500	0.375 ($c_4 = 2$)	0.125
2	2.500	1.500	1.344 ($c_{16} = 6$)	0.156
3	10.500	5.500	5.203 ($c_{64} = 14$)	0.297
4	42.500	21.500	20.518 ($c_{256} = 92$)	0.982

where k is the embedding parameters of DE. For embedding digits in a B-ary notational system using APPM, assume that the probability of replacing (x, y) with each (x', y') in $\Phi_B(x, y)$ is identical. With the knowledge of $\Phi_B(x, y)$, the averaged MSE can be obtained by

$$\begin{aligned}&\mathrm{MSE}_{\mathrm{APPM}} = \frac{1}{2B} \sum_{i=0}^{B-1} \left((x_i - x)^2 + (y_i - y)^2\right) \\ &\text{for } (x_i, y_i) \in \Phi(x, y).\end{aligned} \tag{5}$$

For example, the $\Phi_{16}(x, y)$ that allows concealing digits with the 16-ary notational system is depicted in Fig. 4. The squared distances between $(x_i, y_i) \in \Phi_{16}(x, y)$ and the center position in $\Phi_{16}(x, y)$ are marked in the corresponding positions. The averaged MSE is then calculated by the averaged squared distance

$$\begin{aligned}\mathrm{MSE}_{\mathrm{APPM}(B=16)} &= \frac{1}{2 \times 16}(1 \times 4 + 2 \times 4 + 4 \times 4 + 5 \times 3) \\ &= \frac{43}{32} = 1.344.\end{aligned}$$

LSB and OPAP employ every pixel in the cover image as an embedding unit, and r bits can be embedded into each pixel. Therefore, the payload is r bpp. For the PPM-based embedding method, a payload with r bpp is equivalent to embedding $2r$ bits for every two pixels, which is equivalent to concealing digits in a 2^{2r}-ary notational system. Because DE does not allow embedding digits exactly in a 2^{2r}-ary notational system, we compare the MSE of APPM with LSB and OPAP first. The results are shown in Table II. Note that the results listed in Table II are obtained by using (2)–(5), i.e., the theoretically value of MSE. A very similar result can also be obtained if these methods are applied in nature images.

Table II reveals that the MSE of APPM is smaller than those of LSB and OPAP in all payloads. For example, when the payload is 1 bpp, both OPAP and LSB have the same MSE (MSE $= 0.5$). However, the MSE of APPM is 0.375, which is 1/4 reduction in MSE. For a high payload, e.g., 3 or 4 bpp, the MSE of OPAP is about one half that of LSB; however, the MSE of APPM is decreased by 0.297 and 0.982 for 3 and 4 bpp, respectively, than those of OPAP. Fig. 5 shows the cover image Lena along with the stego images under various payloads. As shown

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

Fig. 5. Cover image and stego images under various payloads. (a) Cover image. (b) Stego image, 2 bpp at 46.86 dB. (c) Stego image, 3 bpp at 40.97 dB. (d) Stego image, 4 bpp at 34.90 dB.

TABLE III
MSE COMPARISON OF THE PROPOSED METHOD WITH CHAO 'S DE METHOD

Base B	bpp	DE		APPM		MSE
		k	MSE	c_B	MSE	Improvement
5	1.161	1	0.4	2	0.4	0
13	1.850	2	1.077	5	1.077	0
25	2.322	3	2.080	5	2.000	0.080
41	2.679	4	3.415	6	3.341	0.074
61	2.965	5	5.082	8	4.902	0.180
85	3.205	6	7.082	10	6.847	0.235
113	3.410	7	9.416	31	9.071	0.345
145	3.590	8	12.083	22	11.890	0.193
181	3.750	9	15.083	39	14.519	0.564
221	3.894	10	18.416	26	17.787	0.629

in the figures, the stego images are visually indistinguishable from the cover images.

The comparison of theoretical MSEs under various payloads for APPM and DE is shown in Table III. Note that for the DE method, only digits in some specific notational system can be concealed, and the notational system used for concealing data is determined by the parameter k. Therefore, we choose $k = 1 \sim 10$ to compare the MSE.

When digits in a 5-ary notational system are embedded ($k = 1$), EMD, DE, and APPM obtain the same MSE because these three methods share the same neighborhood set. When $k \leq 2$, APPM and DE share the same neighborhood set and thus their MSEs are the same. However, when $k > 2$, the MSEs of APPM are lower than those of DE. It is worth mentioning that APPM is capable of embedding digits in any notational system, while DE can only embed digits in $(2k^2 + 2k + 1)$-ary notational system and k must be an integer. Therefore, APPM has the flexibility

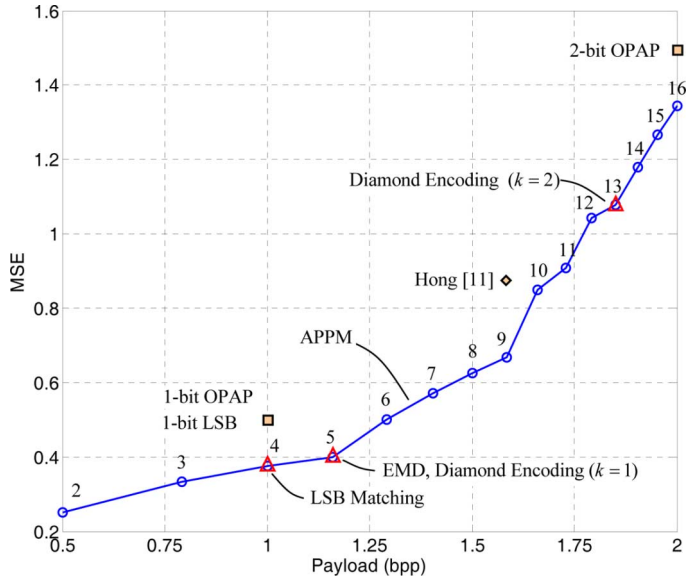

Fig. 6. MSE comparison of various PPM-based methods. The payload-MSE relationship of APPM is denoted by circles. The B-ary digits used for a given payload are marked beside the circle.

TABLE IV
MSE COMPARISON (Payload = 400 000 bits, 1.526 bpp)

Image	2-bit LSB	2-bit OPAP	DE (k=2)	APPM ($c_9 = 3$)
Lena	1.909	1.149	0.888	0.642
Jet	1.905	1.142	0.886	0.648
Boat	1.965	1.145	0.885	0.640
Elaine	1.917	1.138	0.891	0.638
House	1.921	1.147	0.889	0.632
Sailboat	1.904	1.144	0.886	0.641
Average	1.920	1.144	0.887	0.640

to choose a better notational system for data embedding to decrease the image distortion.

Fig. 6 shows the MSE comparison of some PPM-based data-hiding methods for payload less than 2 bpp. It can be seen that the MSEs of APPM are always smaller or equal to other PPM-based methods. For example, when digits in a 4-ary notational system are embedded, the MSEs of APPM and LSB matching are the same. When embedding digits in a 13-ary notational system, APPM and DE ($k = 2$) have the same MSE. However, when embedding 16-ary digits, APPM outperforms OPAP. APPM not only greatly increases the payload of EMD, but also enable users to freely select the desired notational system for data embedding so that a better image quality can be obtained.

B. Comparison of Experimental Results

Six images Lena, Jet, Boat, Elaine, Couple, and Peppers, each sized 512 × 512, are taken as test images to compare the MSE obtained by APPM, OPAP, and DE. The payloads were set to 400 000, 650 000, and 1 000 000, respectively. Message bits were generated by using a pseudorandom number generator (PRNG). The results are shown in Tables IV–VI.

Tables IV–VI reveal that the performance of the proposed APPM method is the best under various payloads. For example, with the payload 400 000 bits, the averaged MSE of 2-bit OPAP is 1.244, whereas the averaged MSE of DE is 0.887. However,

TABLE V
MSE COMPARISON (Payload = 650 000 bits, 2.480 bpp)

Image	3-bit LSB	3-bit OPAP	DE (k=3)	APPM ($c_{32}=7$)
Lena	8.653	4.543	3.154	2.604
Jet	8.638	4.542	3.164	2.609
Boat	8.674	4.552	3.170	2.598
Elaine	8. 728	4.555	3.163	2.582
House	8.871	4.546	3.169	2.600
Sailboat	8.708	4.534	3.159	2.610
Average	8.712	4.545	3.163	2.601

TABLE VI
MSE COMPARISON (Payload = 1 000 000 bits, 3.815 bpp)

Image	4-bit LSB	4-bit OPAP	DE (k=10)	APPM ($c_{199}=37$)
Lena	40.531	20.457	17.991	16.106
Jet	40.530	20.457	18.051	16.113
Boat	40.539	20.527	20.365	16.112
Elaine	40.530	20.498	18.052	16.104
House	40.596	20.456	18.096	16.102
Sailboat	40.583	20.482	19.227	16.108
Average	40.551	20.479	18.63	16.108

the proposed method has the smallest averaged MSE, 0.640. For larger payload, such as 650 000 and 1 000 000 bits, the proposed method also performs better than OPAP and DE because APPM selects the smallest notational system that provides just enough embedding capacity to accommodate the given payload with the least distortion.

V. SECURITY ANALYSIS

The goal of steganography is to evade statistical detection. It is apparent that MSE is not a good measure of security against the detection of steganalysis. For example, low-MSE embedding such as LSB replacement is known to be highly detectable [1], [6]. In this section, we analyze the security of APPM under two statistical steganalysis schemes, including Subtractive Pixel Adjacency Matrix (SPAM) steganalyzer proposed by Pevný *et al.* [19] and the HVDH scheme proposed by Zhao *et al.* [20]. SPAM steganalyzer is a novel Steganographic method for detecting stego images with low-amplitude independent stego signal, while the HVDH scheme is used to detect the presence of hiding message according to the distance between vertical and horizontal histograms. All the test images used in this section are obtained from the UCID [21] and RSP [22] image database, where some literature [13], [23] also adopt this database for their experiments.

A. Security Analysis Under SPAM

SPAM is a modern technique for detecting stego images with independent random stego signal for which typically not found in natural digital images [19]. SPAM obtains the features of images by calculating the transition probabilities along eight directions, and the number of features is determined by the SPAM order and the range of difference T. A soft-margin support vector machine (SVM) with Gaussian kernel is employed to implement the steganalyzer. The error rate

$$P_{\mathrm{Err}} = \frac{1}{2}(P_{\mathrm{Fp}} + P_{\mathrm{Fn}})$$

TABLE VII
MINIMAL ERROR RATE OBTAINED BY SPAM USING UCID IMAGE DATABASE

	0.25 bpp		0.5 bpp	
	LSBM	APPM	LSBM	APPM
1st order SPAM ($T=4$)	0.058	0.310 (4-ary) 0.301 (5-ary) 0.296 (9-ary)	0.023	0.166 (4-ary) 0.191 (5-ary) 0.195 (9-ary)
	LSBM	APPM	LSBM	APPM
2nd order SPAM ($T=3$)	0.039	0.236 (4-ary) 0.243 (5-ary) 0.203 (9-ary)	0.013	0.126 (4-ary) 0.122 (5-ary) 0.123 (9-ary)

TABLE VIII
MINIMAL ERROR RATE OBTAINED BY SPAM USING RSP IMAGE DATABASE

	0.25 bpp		0.5 bpp	
	LSBM	APPM	LSBM	APPM
1st order SPAM ($T=4$)	0.041	0.243 (4-ary) 0.277 (5-ary) 0.235 (9-ary)	0.016	0.173 (4-ary) 0.206 (5-ary) 0.148 (9-ary)
	LSBM	APPM	LSBM	APPM
2nd order SPAM ($T=3$)	0.031	0.199 (4-ary) 0.235 (5-ary) 0.227 (9-ary)	0.012	0.102 (4-ary) 0.133 (5-ary) 0.105 (9-ary)

is calculated to evaluate the security of a data-hiding method against the detection of SPAM, where P_{Fp} and P_{Fn} is the probability of false positive and false negative, respectively. The higher the error rate, the lower the detectability.

To evaluate the detectability of APPM using SPAM, we trained the SPAM steganalyzer on images obtained from UCID and RSP image databases, respectively. UCID consists of 1338 uncompressed images with size 512×384. RSP consists of 10 000 gray-scale images with size 512×512 coming from cropped and resized natural images. The implementation of SPAM features is obtained from [24]. The five-fold cross-validation is employed to compute the classification error. The simulated annealing (SA) optimization is used to find the penalization parameter C and the kernel parameter γ such that the error rate is the lowest.

Because SPAM is effective to detect the ± 1 embedding methods such as LSB matching (LSB-M), which randomly increases or decreases the pixel values by one for matching the LSBs with the message bits, we use the SPAM steganalyzer to detect the APPM in 4-, 5-, and 9-ary notational systems and the LSB-M method with the payloads 0.25 and 0.5 bpp. Note that for both the LSB-M method and APPM with these notational systems, the pixel values of each embedding unit are modified at most by one. The results are shown in Tables VII and VIII, respectively.

As shown in Tables VII and VIII, the error rates obtained by the APPM method are significantly higher than those obtained by the LSB-M, indicating that APPM is less detectable than LSB-M under the same payload. For example, for the UCID image database with payload 0.25 bpp, the error rate of LSB-M using the second-order SPAM is 0.039, while the error rate of APPM with a 5-ary notational system is 0.243. The undetectability is significantly higher than that of LSB-M. Experiments on the RSP image database also revealed similar

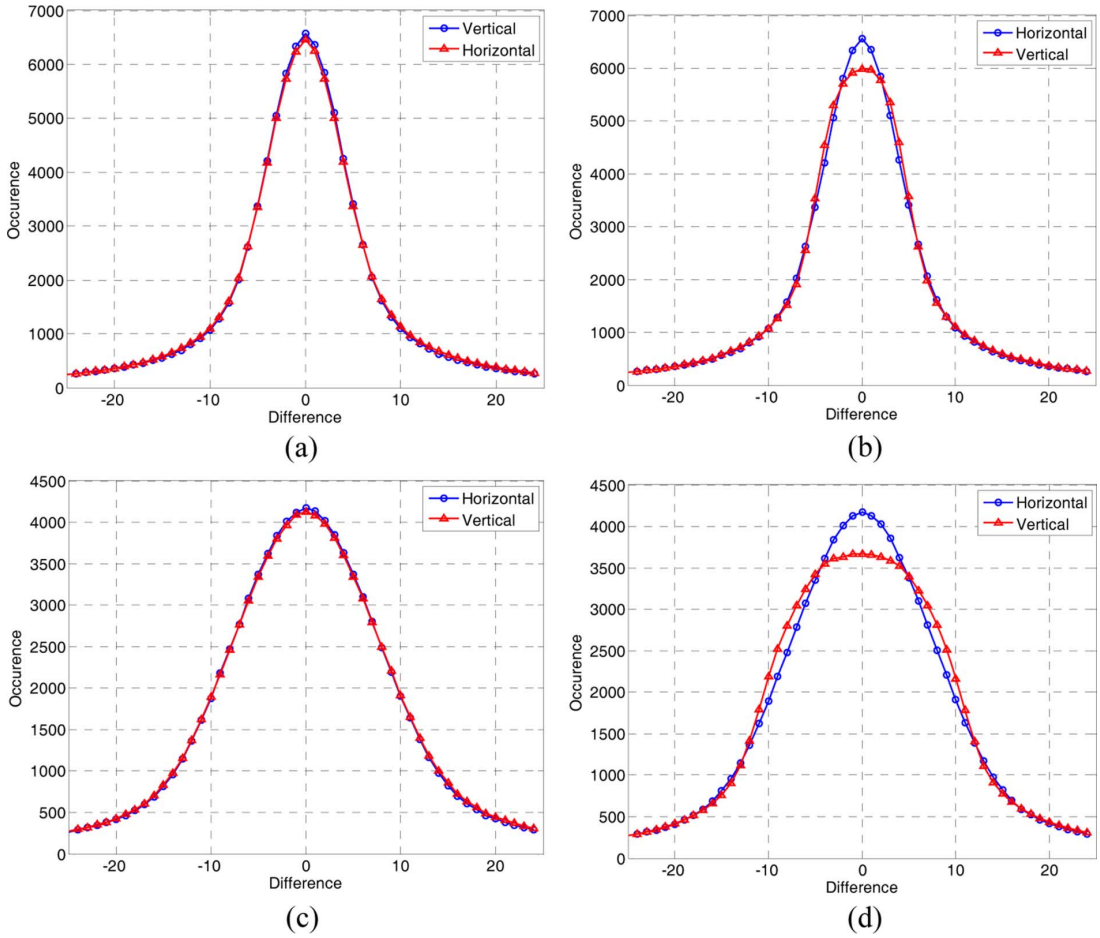

Fig. 7. Comparison of the averaged vertical and horizontal difference histograms of APPM and DE. (a) AMMP ($c_{53} = 8$), $D = 131$ (53-ary notational system). (b) DE ($k = 5$), $D = 937$ (53-ary notational system). (c) AMMP ($c_{221} = 26$), $D = 189$ (221-ary notational system). (d) DE ($k = 10$), $D = 1449$ (221-ary notational system).

results. The experimental results agree with the fact that APPM is more secure against SPAM steganalyzer than LSB-M.

B. Statistical Analysis of the Histogram Differences

In 2009, Zhao *et al.* [20] proposed a detection method based on the statistical analysis of histogram differences. Zhao *et al.* observed that for many pairwise embedding methods, the difference between the horizontal difference histograms $\hat{H}_h$ and vertical difference histograms $\hat{H}_v$ are significantly altered. Zhao *et al.* use the distance between $\hat{H}_h$ and $\hat{H}_v$ as a statistical detector to detect the abnormality of histogram. The distance is defined as

$$D = \left(\sum_{i=-2T}^{2T} \left(\hat{H}_h(i) - \hat{H}_v(i) \right) \right)^{1/2}$$

where T is a predefined threshold. A larger D indicates that $\hat{H}_h$ and $\hat{H}_v$ have larger differences and thus, the image is likely to have messages embedded. We compare APPM with DE at high payload because the abnormality of histograms often occurs when the payload is high. In the experiment, we randomly selected 100 images from [21], and averaged the horizontal and vertical difference histograms of the stego images obtained by APPM and DE. We chose the embedding parameter $k = 5$ and $k = 13$ for DE, which were equivalent to embed digits in 53-ary and 221-ary notational systems, respectively. Digits in the same notational systems were used in APPM. All the test images were fully embedded, and $T = 20$ was used in the experiments, as suggested in [20]. The results are shown in Fig. 7.

As can be seen in Fig. 7(a) and (c), the averaged horizontal and vertical difference histograms obtained by APPM are almost the same ($D = 131$ and 189, respectively), whereas the difference histograms shown in Fig. 7(b) and (d) obtained by DE are significantly altered ($D = 937$ and 1449, respectively). The results show that APPM preserves the shape of difference histogram even at high payload, which indicates that the proposed method is secure under Zhao *et al.*'s method. On the other hand, DE deviates the distance between the horizontal and vertical histograms significantly, and the presence of the embedded message is likely to be detected.

VI. Conclusion

This paper proposed a simple and efficient data embedding method based on PPM. Two pixels are scanned as an embedding unit and a specially designed neighborhood set is employed to embed message digits with a smallest notational system. APPM allows users to select digits in any notational system for data embedding, and thus achieves a better image quality. The proposed

method not only resolves the low-payload problem in EMD, but also offers smaller MSE compared with OPAP and DE. Moreover, because APPM produces no artifacts in stego images and the steganalysis results are similar to those of the cover images, it offers a secure communication under adjustable embedding capacity.

REFERENCES

[1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, pp. 727–752, 2010.

[4] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in *Proc. SPIE, Media Forensics and Security*, 2010, vol. 7541, DOI: 10.1117/12.838002.

[5] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 111–119, Mar. 2006.

[6] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Int. Workshop on Multimedia and Security*, 2001, pp. 27–30.

[7] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

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

[9] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[10] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.

[11] W. Hong, T. S. Chen, and C. W. Shiu, "A minimal Euclidean distance searching technique for Sudoku steganography," in *Proc. Int. Symp. Information Science and Engineering*, 2008, vol. 1, pp. 515–518.

[12] R. M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[13] J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "An improved section-wise exploiting modification direction method," *Signal Process.*, vol. 90, no. 11, pp. 2954–2964, 2010.

[14] W. Zhang, X. Zhang, and S. Wang, "A double layered plus-minus one data embedding scheme," *IEEE Signal Process. Lett.*, vol. 14, no. 11, pp. 848–851, Nov. 2007.

[15] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pt. 2, pp. 3923–3935, Oct. 2005.

[16] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Proc. SPIE, Security, Steganography., Watermarking of Multimedia*, 2007, vol. 6050, pp. 2–3.

[17] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 390–394, Sep. 2006.

[18] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognit.*, vol. 41, no. 8, pp. 2674–2683, 2008.

[19] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[20] H. Zhao, H. Wang, and M. K. Khan, "Statistical analysis of several reversible data hiding algorithms," in *Proc. Multimedia Tools and Applications*, 2009, DOI: 10.1007/s11042-009-0380-y.

[21] UCID image database [Online]. Available: http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html

[22] RSP image database [Online]. Available: http://dud.inf.tu-dresden.de/westfeld/rsp/rsp.html

[23] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," *J. Vis. Commun. Image Represent.*, vol. 22, no. 2, pp. 131–140, 2011.

[24] Implementation of the SPAM features [Online]. Available: http://dde.binghamton.edu/download/spam/

Wien Hong received the M.S. and Ph.D. degrees from the State University of New Your at Buffalo, in 1994 and 1997, respectively.

From 1999 to 2009, he was an assistant professor in the Department of Information Management, Yu-Da College of Business, Taiwan. Since November 2009, he has been an associate professor in the Department of Information Management, Yu-Da University, Taiwan. His research interests include digital watermarking, data hiding, and data compression.

Tung-Shou Chen received the B.S. and Ph.D. degrees from National Chiao Tung University, in 1986 and 1992, respectively, both in computer science and information engineering.

From 1994 to 1997, he was with the faculty of the Department of Information Management, National Chin-Yi Institute of Technology, Taiwan. From 1998 to 2000, he was both the Dean of Student Affairs and a professor in the Department of Computer Science and Information Management, Providence University, Taiwan. Since August 2000, he has been a professor in the Graduate School of Computer Science and Information Technology, National Taichung Institute of Technology, Taiwan. From 2004 to 2007, he was also the dean of the Graduate School of Computer Science and Information Technology, National Taichung Institute of Technology. His current research interests include data mining, image cryptosystems, and image compression.