On Security Improvement of Adaptive Pixel Pair Matching with Modified Searching Mechanism

Wien Hong[1,2], Shuozhen Zheng[1], and Xiaoyu Zhou[1]
(Corresponding author: Wien Hong)

School of Electrical and Computer Engineering, Nanfang College of Sun Yat-Sen University[1]
882 Wenquan Rd. Conghua district, Guangzhou 510970, China
School of Computer and Software, Nanjing University of Information Science and Technology[2]
219 Niliu Rd. Nanjing, Jiangsu 210044, China
(Email: wienhong@gmail.com)

(Received Oct. 16, 2017; revised and accepted Mar. 27, 2018)

Abstract

This paper proposes a data hiding scheme that improves the adaptive pixel pair matching (APPM) method. Based on pixel pair matching, APPM employs a pixel pair as an embedding unit, and uses a specially designed reference table that minimizing the embedding distortion for data embedment. Although APPM has the capability to embed secret digit in any notational system, it is vulnerable to the detection by the RS scheme if digits in 4-ary notational system are embedded into images with large flat area (pixels having the similar grayscale values) such cartoon images. A modified version of APPM is proposed in this paper by using a revised pixel pair replacement mechanism (PPRM). With the proposed PPRM method, the stego image not only is totally undetectable by the RS scheme but also provides the equivalent image quality of the original APPM method.

Keywords: APPM; Data Hiding; Pixel Pair Matching

1 Introduction

The simple LSB substitution technique is a commonly used data hiding method in which least significant bits of pixels are replaced by secret data. The LSB method is easy to implement, and achieves an acceptable image quality. Therefore, it is widely used in many applications such as data hiding, watermarking, and image authentication [1,6,9,14,15,17,19,21–23]. However, during the LSB embedment, pixels with odd values remain unchanged or subtracted by one, and pixels with even values remain unchanged or add by one. As a result, the unbalanced replacement significantly increases the detectability by the steganalyzers such as RS scheme [7]. Moreover, The LSB method distorts the image significantly. Therefore, it is not suitable for applications where a high image quality is demanded [7,13,16].

In 2004, Chan *et al.* [2] proposed a simple but efficient data hiding method by using optimal pixel adjustment process (OPAP). When secret data are embedded into the rightmost r LSBs, the OPAP method employs a simple adjustment for the leftmost $8-r$ bits such that the stego pixel value is the closest to its original pixel value. The OPAP method has the same payload as the LSB method but provides better image quality. However, the OPAP method has the equivalent distortion compared to that of the LSB method when the payload is 1 bit per pixel (bpp).

Both LSB and OPAP employ a single pixel as an embedding unit for data embedment. Another type of data hiding method utilizes a pixel pair as an embedding unit to embed a n-ary digit. Data hiding method of this type are termed pixel pair matching (PPM). The PPM-based method uses a reference table as a guide, and embeds a digit into a pixel pair by modifying pixel values of this pair. For example, to embed a digit d_B in base B into a pixel pair (r, c) using a reference table R_T, the coordinate (r, c) in R_T is firstly located and obtain a searching region $\Omega(r, c)$. In this region, a coordinate (r', c') is found which satisfies $R_T(r', c') = d_B$ and is the closest to (r, c). The pixel pair (r, c) is then replaced by the new coordinate (r', c'). The embedded digits d_B can be extracted by locating the element at coordinate (r', c') of the given reference table R_T, *i.e.*, $d_B = R_T(r', c')$. Figure 1 shows the schematic diagram of the PPM-based method.

Mielikainen [18] in 2006 proposed a LSB matching revisited (LSBMR) method based on PPM. In his method, only one pixel in a pixel pair is changed by one grayscale unit and two bits (a 4-ary digit) can be embedded into this pixel pair. The mean square error (MSE) cause by data embedding using LSBMR is 0.375 [18], which is significantly smaller than that of LSB (0.5). In the same year, Zhang and Wang [24] proposed an exploiting modification direction (EMD) method to enhance the embedding efficiency of LSBMR. EMD embeds a 5-ary digit into a pixel pair but only modifies one pixel one grayscale unit at most. Although EMD provides a better embedding efficiency and lower detectability, the payload is limited to 1.161 bpp at most.

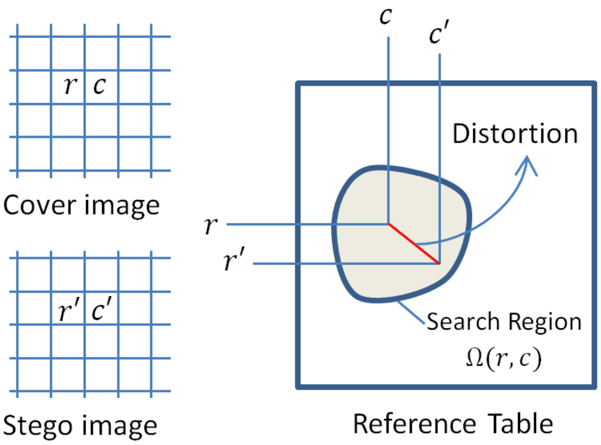


Figure 1: Illustration of the PPM method

In 2008, Chang *et al.* [3] proposed a data hiding method based on solutions of Sudoku tables to increase the payload of EMD. Later, Hong *et al.* [11, 12] modified the searching algorithm of [3] to further increase the image quality by 1.8 dB under the same payload. Chao *et al.* [4] in 2009 proposed a diamond encoding (DE) method with extensible payload. DE embeds a digit in B-ary notational system into a pixel pair, where $B = 2k^2 + 2k + 1$ and k is an integer. When $k = 1$, the embedding performance of DE is equivalent to that of EMD.

In 2012, Hong and Chen [10] proposed an adaptive pixel pair matching (APPM) method to further enhance the embedding performance of PPM based method. Compared to DE method, APPM embeds digits in any notational system but DE embeds digits only in base $2k^2 + 2k + 1$. Since the MSE caused by pixel pair replacement in APPM method are minimized, APPM always achieves a higher image quality under the same payload with lower detectability compared to other PPM-based methods. Although APPM embeds digit in any notational system, it is likely detectable when using RS scheme [7] if 4-ary secret digits are embedded into the image containing larger flat area such cartoon images. Some recent works [5, 8, 20] have exploited the merit of the APPM and developed state-of-the-art works for hiding data. However, the vulnerability to the detection by the RS scheme is yet unsolved.

In this paper, a data hiding method that modified APPM's embedding method by stochastically selecting embeddable positions is proposed. The proposed method not only maintains the same image quality but also provides a smaller detectability than that of APPM method. The rest of this paper is organized as follows. Section 2 is the proposed method, while Section 3 gives the experimental results and discussions. Concluding remarks are given in Section 4.

2 The Proposed Method

In the PPM-based method, the embedding performance is greatly influenced by the design of reference table. In general, a reference table can be constructed by patches or using a formula. APPM use the function

$$R_T(r, c) = (r + c_B \times c) \bmod B$$

to construct the reference table, where c_B is the embedding parameter for B-ary reference table. The reference table used in APPM can be divided into patches (search region) such that the MSE caused by pixel pair replacement is minimized. The embedding parameter used in APPM method for B-ary is listed in Table 1. More details about the obtaining of c_B can be seen in [10].

Although APPM performs the best compared to the existing PPM-based method, it is likely to be detectable by RS scheme [7] when cover images contain large flat area with 4-ary digits are embedded. The flat area in images represents pixels in that area having the similar grayscale values and the cartoon images are often of this type. When APPM are applied on pixels in flat area, APPM's embedding algorithm will confined a search region such that one pixel in a pixel pair will always be added or subtracted by one when embedding a certain 4-ary digit. In this circumstance, it is likely to be detected by the RS scheme.

In this section, a method to secure APPM's embedding method is proposed by evading the RS detection. To do this, if there are two candidates satisfying $R_T(r', c') = d_B$ and are both the nearest to (r, c), then one of them is randomly selected to replace the original pixels. With the aid of random selection, different candidates will be selected and thus the stego image can evade the RS detection. Note that the proposed method can be applied on both the natural images or artificial images such as cartoon images.

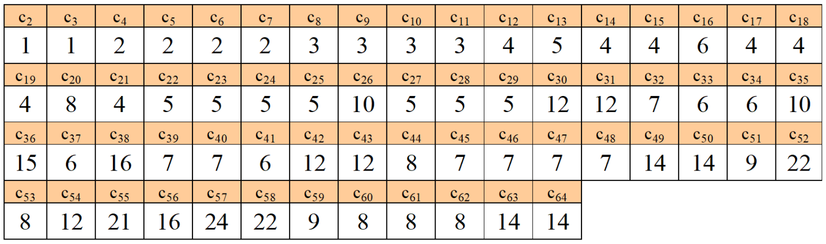
2.1 Embedding Procedures

Let I be the cover image of size $M \times M$, and S be the set of B-ary secret digits to be embedded. Firstly, a reference table R_T is constructed according to the extraction function. Then, the pixel pairs in the cover image are scanned and secret digits are embedded into the scanned pixel pairs. The detailed embedding procedures are listed below.

Input: Cover image of size $M \times M$, embedding parameter c_B, and B-ary secret digits S.

Output: Stego image.

Step 1: Construct the reference table R_T for embedding B-ary secret digits using the function $R_T(r, c) = (r + c_B \times c) \bmod B$.



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	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					

Figure 2: Embedding parameter c_B used in APPM

Step 2: Extract a secret digit s_B from S.

Step 3: Scan the pixels in the cover image using the raster scan order. Let the pixels pair (r, c) be the scanned pixels.

Step 4: In the reference table R_T, find all the coordinates (r', c') satisfying $R_T(r', c') = s_B$ and having the smallest L, where $L = (r' - r)^2 + (c' - c)^2$. If there are more than one pixel pair satisfying the above two conditions, randomly choose a pair $(\hat{r}', \hat{c}')$ and then replace the original pair (r, c) by $(\hat{r}', \hat{c}')$.

Step 5: Repeat Steps 2–4 until all the secret data are embedded.

2.2 Extraction Procedures

To extract the embedded secret digits, the receiver obtains the information about c_B and B via a secret channel, and then performs the data extraction. The detailed extraction procedures are listed below.

Input: Stego image, the parameter c_B and B.

Output: Secret data S.

Step 1: Construct the reference table R_T which is identical to the one used in the embedding procedure.

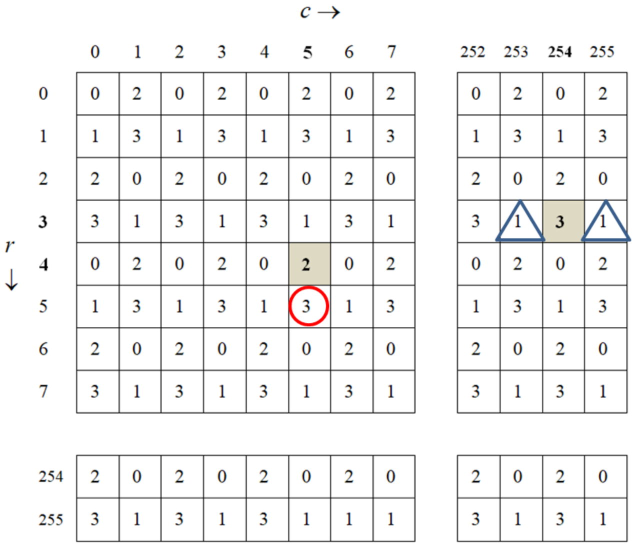
Step 2: Scan the pixel pairs in the stego image using the raster scan order. Let the scanned pixel pair be (r', c'). The embedded secret digit can be easily extracted by using the equation $s_B = R_T(r', c')$

Step 3: Repeat Step 2 until all the secret digits are extracted.

2.3 A Complete Example

In this section, an example is used to illustrate the proposed method. Let {(3,254),(4,5)} be a set of cover pixel pairs and two 4-ary digits ($B = 4$) to be embedded into these pixel pair are $S = \{1_4, 3_4\}$. From Figure 2, the embedding base $c_B = 2$ can be obtained. The reference table R_T can be constructed using $f(r, c) = (r + 2 \times c) \bmod 4$. For example, the entity located in the zeroth row and the fifth column is $f(0, 5) = (0 + 2 \times 5) \bmod 4 = 2$, and the entity located in the fifth row and the third column is $f(5, 3) = (5 + 2 \times 3) \bmod 4 = 3$. The constructed table is partially shown in Figure 3. The first scanned cover pixel pair is $(3, 254)$ and the secret data to be embedded is $s_4 = 1_4$. The position located at $(3, 254)$ in the reference table is shaded gray, as shown in Figure 3. Since $(3, 253)$ and $(3, 255)$ (marked by triangles) are both the closest coordinate to $(3, 254)$ and $R_T(3, 253) = R_T(3, 255) = 1_4$, a pixel pair is randomly selected to replace $(3, 254)$. Suppose the selected pair is $(3, 253)$, and thus the pixel pair $(3, 253)$ is used to replace the original pixel pair $(3, 254)$. Next, the second pixel pair $(4, 5)$ is visited and the secret data to be embedded is $s_4 = 3_4$. Since $(5, 5)$ is the closet coordinate (marked by a circle) to $(4, 5)$ while satisfying $R_T(5, 5) = 3_4$, the cover pixel pair $(4, 5)$ is then replaced by $(5, 5)$. Therefore $(r', c') = (5, 5)$ is obtained. As a result, the set of stego pixel pair is $\{(3, 253), (5, 5)\}$.

To extract the embedded digits from the stego pixel pair $(3, 253), (5, 5)$, the reference table is firstly constructed, as in the embedding phase. Because $R_T(3, 253) = 1$, a secret digit $s_4 = 1_4$ is extracted. Similarly, Because $R_T(5, 5) = 3$, a secret digit $s_4 = 3_4$ is extracted.

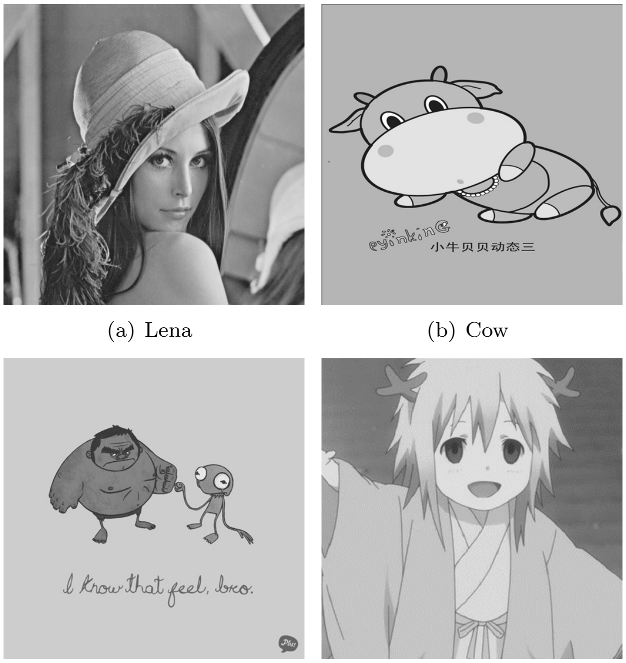


	0	1	2	3	4	5	6	7	252	253	254	255
0	0	2	0	2	0	2	0	2	0	2	0	2
1	1	3	1	3	1	3	1	3	1	3	1	3
2	2	0	2	0	2	0	2	0	2	0	2	0
3	3	1	3	1	3	1	3	1	3	1	3	1
4	0	2	0	2	0	2	0	2	0	2	0	2
5	1	3	1	3	1	3	1	3	1	3	1	3
6	2	0	2	0	2	0	2	0	2	0	2	0
7	3	1	3	1	3	1	3	1	3	1	3	1
254	2	0	2	0	2	0	2	0	2	0	2	0
255	3	1	3	1	3	1	1	1	3	1	3	1

Figure 3: Reference table used in the example

3 Experimental Results

In this section, several tests are performed to demonstrate the applicability of the proposed method and compared the results with those of the original APPM method. Four 8-bit grayscale test images, including Lean, Cow, Giant, and Kid, each of size 512 × 512, are used in the experiments, as shown in Figure 4. Among these test images, the Lena image is a natural image and others are cartoon images. These cartoon images all contain large flat areas in which pixels and their neighbors have similar grayscale values. The pseudo random number generator is used to generate 4-ary secret digits. The PSNR metric is used to measure the image quality.



(a) Lena (b) Cow

(c) Giant (d) Kid

Figure 4: Four test images

3.1 Image Quality Comparison

In this section, the image qualities obtained by the proposed and the APPM methods are compared. The results are shown in Table 1. Table 1 shows that proposed method does not degrade image quality comparing to that of APPM and still offers a very satisfactory image quality.

Table 1: Comparisons of PSNR

Image	APPM	PPRM
Lena	52.39	52.39
Cow	52.38	52.39
Giant	52.38	52.38
Kid	52.38	52.38

3.2 RS Scheme Steganalysis

In this section, the RS scheme is used to detect the stego images obtained from the proposed method and the APPM method. RS scheme partitions images into groups G of n consecutive pixels, and use a discrimination function and a mask M to classify G into three disjoint groups, namely regular, singular and unusable groups. The ratios of the regular groups R_{+M}, R_{-M} and singular groups S_{+M}, S_{-M} are then calculated. In general, if the LSBs of an image are not embedded, the relationships $R_{+M} \simeq R_{-M}$ and $S_{+M} \simeq S_{-M}$ generally hold. Otherwise, the difference between them will be increased as the embedding rate is increased. In the experiments,

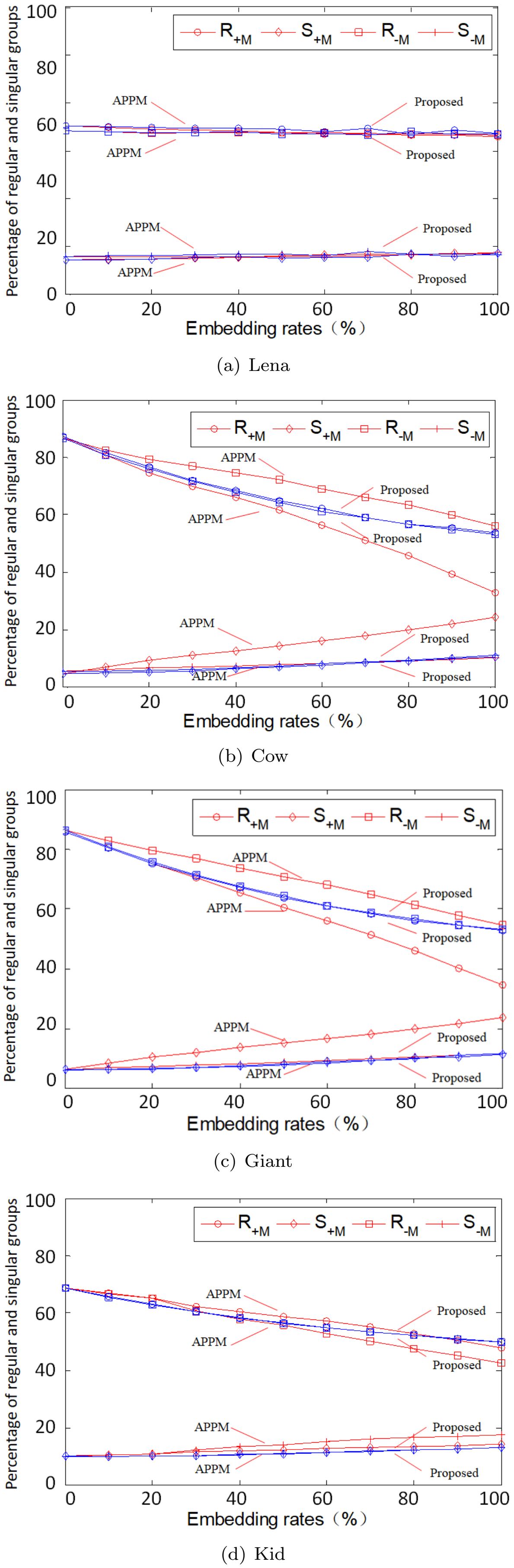
$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is used as the mask matrix. The results are shown in Figure 5.

Note that for the Lena image, the RS scheme cannot detect the presence of the embedment of the proposed PPRM and the APPM methods because R_{+M} and R_{-M} are indistinguishable and so do S_{+M} and S_{-M}. However, for the test images Cow, Giant and Kid, the differences between R_{+M} , R_{-M} and S_{+M} , S_{-M} increase in the APPM method as the embedding rates increases, indicating that the presence of embedment is more detectable at larger payload. For example, when the embedding rate is 100% (fully embedded), $R_{+M} \simeq 32\%$ and $R_{-M} \simeq 58\%$ are obtained. The difference between them is 26%. The large difference shows that the image is more likely an embedded one. On the other hand, R_{+M} and R_{-M} of the proposed method are both close to 57% even when the embedding rate is 100%, and S_{+M} and S_{-M} also have the similar trends. Therefore, the proposed method is more likely undetectable using the RS scheme. Experiments on other test images also show the similar results, indicating that the proposed method effectively resists the RS attack while providing a very satisfactory image quality.

4 Conclusions

In this paper, a more secure data hiding method by modifying the embedding method of APPM is proposed. During embedding, if the candidates of pixel pairs are more than one, one of them is randomly selected to replace the original pixel pair. The modified pixel pair selection successfully randomizes the replacement to avoid always selecting the same candidates. Compared to the original APPM, the proposed method is undetectable by RS scheme without sacrificing the image quality. The proposed work can be utilized as an embedding method for digital watermarking or image authentication, since the embedding distortion is lower than those of LSB or LSB matching while providing an adjustable payload. The future work will be extended to include more pixels as an embedding unit to conceal data bits while minimizing the distortion.



(a) Lena

(b) Cow

(c) Giant

(d) Kid

Figure 5: RS detection results of four test images

References

[1] J. Bai, C. C. Chang, T. S. Nguyen, C. Zhu, and Y. Liu, "A high payload steganographic algorithm based on edge detection," *Displays*, vol. 46, pp. 42-51, 2017.

[2] 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.

[3] C. C. Chang, Y. C. Chou, and T. D. Kieu, "An information hiding scheme using sudoku," in *3rd International Conference on Innovative Computing Information and Control*, pp. 17–17, June 2008.

[4] R. M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP Journal on Information Security*, vol. 2009, pp. 658047, May 2009.

[5] J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," *Signal Processing: Image Communication*, vol. 29, no. 3, pp. 375–384, 2014.

[6] H. Dadgostar and F. Afsari, "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified lsb," *Journal of Information Security and Applications*, vol. 30, pp. 94-104, 2016.

[7] J. Fridrich, M. Goljan, and R. Du, "Detecting lsb steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, pp. 22–28, Oct. 2001.

[8] W. Hong, "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique," *Information Sciences*, vol. 221, pp. 473–489, 2013.

[9] W. Hong, M. Chen, and T. S. Chen, "An efficient reversible image authentication method using improved pvo and lsb substitution techniques," *Signal Processing: Image Communication*, vol. 58, pp. 111-122, 2017.

[10] W. Hong and T. S. Chen, "A novel data embedding method using adaptive pixel pair matching," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 176–184, Feb. 2012.

[11] W. Hong, T. S. Chen, and C. W. Shiu, "A minimal euclidean distance searching technique for sudoku steganography," in *International Symposium on Information Science and Engineering*, vol. 1, pp. 515–518, Dec. 2008.

[12] W. Hong, T. S. Chen, and C. W. Shiu, "Steganography using sudoku revisited," in *Second International Symposium on Intelligent Information Technology Application*, vol. 2, pp. 935–939, Dec. 2008.

[13] 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.

[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] M. Juneja and P. S. Sandhu, "Improved LSB based steganography techniques for color images in spatial domain," *International Journal of Network Security*, vol. 16, pp. 452–462, 2014.

[16] A. D. Ker, "Steganalysis of lsb matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12, no. 6, pp. 441–444, 2005.

[17] S. Manoharan, D. RajKumar, "Pixel value differencing method based on CMYK colour model," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 37–46, 2016.

[18] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, pp. 285–287, May 2006.

[19] S. Rajendran and M. Doraipandian, "Chaotic map based random image steganography using LSB technique," *International Journal of Network Security*, vol. 19, pp. 593–598, 2017.

[20] S. Y. Shen and L. H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Computers & Security*, vol. 48, pp. 131–141, 2015.

[21] Y. L. Wang, J. J. Shen, and M. S. Hwang, "An improved dual image-based reversible hiding technique using lsb matching," *International Journal of Network Security*, vol. 19, pp. 858–862, 2017.

[22] Y. L. Wang, J. J. Shen, M. S. Hwang, "A novel dual image-based high payload reversible hiding technique using LSB matching", *International Journal of Network Security*, vol. 20, no. 4, pp. 801–804, 2018.

[23] H. C. Wu, N. I Wu, C. S. Tsai, M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEE Proceedings Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611–615, 2005.

[24] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, pp. 781–783, Nov. 2006.

Biography

Wien Hong received his M.S. and Ph.D. degree from the State University of New York at Buffalo, USA in 1994 and 1997, respectively. He is currently a researcher at Taiwan development Institute, and Nanjing University of Information Science and Technology. He is also a professor in the School of Electrical and Computer Engineering at Nanfang College of Sun Yat-Sen University. His research interests include steganography, watermarking and image compression.

Shuozhen Zheng is a senior researcher and engineer at School of Electrical and Computer Engineering, Nanfang College of Sun Yat-Sen University since 2013. He has incorporate several major projects about digital signal processing (DSP) and applications of embedded system. His research interests include development of single-chip microcomputer, image compression, data hiding, and image authentication.

Xiaoyu Zhou jointed the research team of information security in Nanfang College of Sun Yat-Sen University since 2016. She has independently completed several projects in the field of electrical and computer engineering, including digital watermarking and pattern recognition. Her research interests include computer vision and image authentication.