Hindawi
Advances in Multimedia
Volume 2018, Article ID 7682098, 8 pages
https://doi.org/10.1155/2018/7682098

Research Article

A Formula Adaptive Pixel Pair Matching Steganography Algorithm

Min Long [1,2] **and Fenfang Li** [1]

[1] *College of Computer and Communication Engineering, Changsha University of Science and Technology, 410114, China*
[2] *Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation, Changsha University of Science and Technology, Changsha, Hunan Province 410114, China*

Correspondence should be addressed to Min Long; caslongm@aliyun.com

Received 23 January 2018; Revised 31 March 2018; Accepted 30 April 2018; Published 5 July 2018

Academic Editor: Mehdi Hussain

Pixel pair matching (PPM) is widely used in digital image steganography. As an important derivation, adaptive pixel pair matching method (APPM) offers low distortion and allows embedded digits in any notational system. However, APPM needs additional space to store, calculate, and query neighborhood set, which needs extra cost. To solve these problems, a formula adaptive pixel pair matching (FAPPM) method is proposed in this paper. The basic idea of FAPPM is to use the formula to get the stego image pixel pair without searching the neighborhood set for the given image pixel pair. This will allow users to embed secret message directly without storing and searching the look-up table. Experimental results and analysis show that the proposed method could embed secret data directly without searching the neighborhood sets by using a formula and it still maintains flexibility in the selection of notional system, high image quality, and strong anti-steganalysis ability.

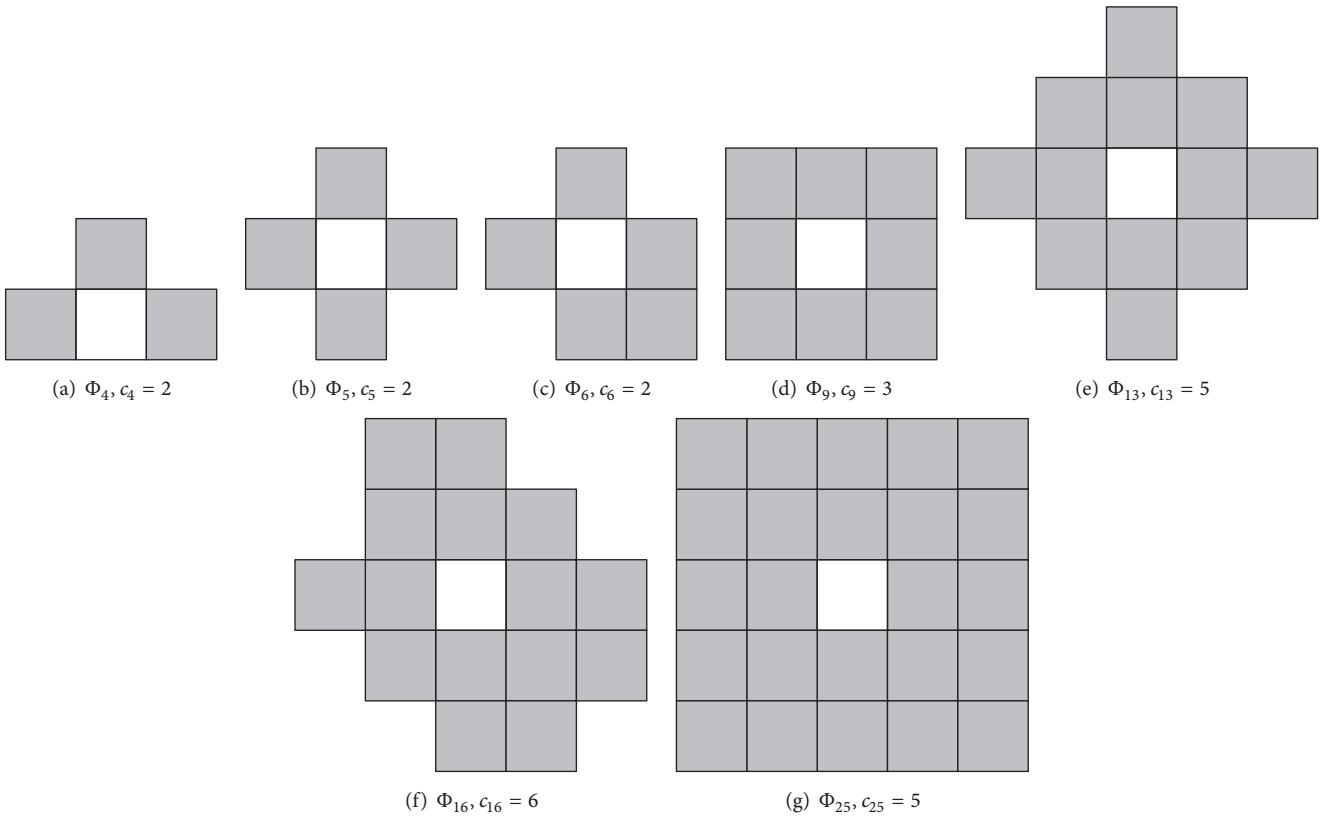
1. Introduction

Information hiding is a technology of embedding secret data into the media for covert communication [1]. With the rapid development of Internet, a large number of data are transmitted over the Internet. At present, the main media using for data hiding includes images, audio, and video, where digital image is the most widely used media [2]. Researchers have shown a great interest in image steganography for the last decade [3]. LSB replacement [4] is one of the most commonly used steganographic techniques, which makes full use of the characteristics that the human visual system is not sensitive to small changes in pixels and the negligible contribution of the low bit plane of the pixel to the image quality. However, this method can only add 1 or remain unchanged for the even pixels and can only decrease 1 or remain unchanged for the odd pixels. Therefore, this unbalanced embedding distortion leads to the histogram attack to the images [5, 6]. Chan et al. [7] proposed an optima pixel adjustment process (OPAP) method, which adjusted the pixels to reduce the distortion caused by least significant bit (LSB) embedding. The LSB and OPAP methods both employed one pixel as an embedding unit to embed secret message. As the development of steganography, methods using two or more pixels as a basic unit for B-ary secret information embedding were put forward. This kind of stenographic algorithm can improve the embedding capacity and image quality by subtle modifying the pixel.

In 2006, Miekikainen [11] proposed a LSB matching method. It employed two pixels as embedding unit. In this method, when payload was 1 bit per pixel, the mean square error (MSE) is 0.375, while the MSE of LSB [4] was 0.5. Zhang and Wang [12] proposed exploiting modification direction (EMD) method, which added and subtracted 1 in one pixel and embedded $2n + 1$-ary secret message in n pixels. When $n = 2$, a quinary number was embedded in each pair of pixels. The capacity can reach the maximum $(1/2)\log_2 5 = 1.161$ bit per pixel (bpp). Chao et al. [13] extended this method and proposed a diamond encoding (DE) method. It can embed $2k^2+2k+1$-ary information to each pair of pixels and achieve high embedding efficiency by adding and subtracting 1 operation in n pixels. In [8], the author used a codebook to

Table 1: Extraction Function Coefficient c_B of APPM.

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}
1	1	2	2	2	2	3	3	3	3	4	5	4	4	6
c_{17}	c_{18}	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}
4	4	4	8	4	5	5	5	5	10	5	5	5	12	12
c_{32}	c_{33}	c_{34}	c_{35}	c_{36}	c_{37}	c_{38}	c_{39}	c_{40}	c_{41}	c_{42}	c_{43}	c_{44}	c_{45}	c_{46}
7	6	6	10	15	6	16	7	7	6	12	12	8	7	7
c_{47}	c_{48}	c_{49}	c_{50}	c_{51}	c_{52}	c_{53}	c_{54}	c_{55}	c_{57}	c_{58}	c_{59}	c_{60}	c_{61}	c_{62}
7	7	14	14	9	22	8	12	21	16	24	22	9	8	8
c_{63}	c_{64}													
14	14													



(a) $\Phi_4, c_4 = 2$ (b) $\Phi_5, c_5 = 2$ (c) $\Phi_6, c_6 = 2$ (d) $\Phi_9, c_9 = 3$ (e) $\Phi_{13}, c_{13} = 5$

(f) $\Phi_{16}, c_{16} = 6$ (g) $\Phi_{25}, c_{25} = 5$

Figure 1: Neighborhood set (shaded region) for APPM.

improve the EMD scheme, and one secret (2^{n+x}-1)-ary digit was hidden in a group of pixels in an image as a modified secret digit. In [9], the authors proposed a method to modify a group of pixels by ±1 to embed a secret digit, but it is only applicable to 3^n-ary notational system. Kuo et al. [14] proposed a formula diamond encoding (FDEMD) data hide scheme, and it could conceal a digit in $(2k^2+2k+1)$-ary system. It simplified the embedding procedure and embedded secret data without storing and calculating characteristic value matrix. Hong et al. [10] designed a new extraction function and new neighborhood set of two pixels called adaptive pixel pair matching (APPM). It allowed embedding digits in arbitrary notational system and the distortion caused by embedment using APPM was minimized; therefore the resultant marked image quality could be well preserved [15]. In [16], secure adaptive pixel pair matching (SAPPM) was proposed to hide multiple data types such as text, image, and audio which incorporated cryptography along with steganography. A transformed version of adaptive pixel pair matching (APPM) was used for image steganography to get lower distortion [17]. However, APPM need to calculate, store, and query the modified neighborhood set table.

Based on the above methods, this paper simplifies the embedding procedure and designs an extraction function to construct a formula adaptive pixel pair matching (FAPPM) method. It does not need to calculate, store, and query the

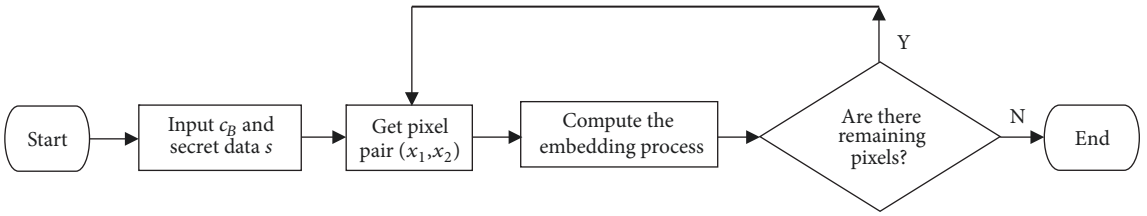


Figure 2: The embedding process.

Input: A pixel pair (x_1, x_2), extraction function coefficient c_B and secret data s.
Output: Stego pixel pair (x_1', x_2').
Step 1: Set $f = (x_1 + c_B x_2) \bmod B$
Step 2: Set $k = \lceil (\lceil \sqrt{B} \rceil - 1)/2 \rceil$
Step 3: Set $D = s - f$
Step 4: If $D < 0$ then $D = D + B$
Step 5: Set $next\_t_1 = |D| \bmod c_B$
Step 6: While $i = 1$ to 4 do
  Set $t_1 = next\_t_1$
  Set $t_2 = (D - t_1)/c_B$
  If $|t_1| \le k \&\& |t_2| \le k$ then
    Set $x_1' = x_1' + t_1$
    Set $x_2' = x_2' + t_2$
  Else
    Switch (i)
      Case 1:
        Set $next\_t_1 = t_1 - c_B$
      Case 2:
        Set $D = D - B$
        Set $next\_t_1 = -(|D| \bmod c_B)$
      Case3:
        Set $next\_t_1 = t_1 + c_B$
      Case4:
        Print "Error"
    End Switch
  End if
End While

Algorithm 1

modified neighborhood set table, and it can realize the data hiding in any notional system.

2. A Review of Adaptive Pixel Pair Matching (APPM)

The APPM method [10] used a pair of pixels (x, y) as a coordinate, where an extraction function $f_{APPM}(x, y)$ was designed. Then a neighborhood set $\Phi(x, y)$ of (x, y) was established.

$$f_{APPM}(x, y) = (x + c_B y) \bmod B \quad (1)$$

where $f(x, y)$ and $\Phi(x, y)$ satisfied the following three conditions:

(i) In the neighborhood set $\Phi(x, y)$, there are exactly B pairs of coordinates.

(ii) In the neighborhood set $\Phi(x, y)$, the extracted function values for each coordinate are mutually exclusive.

(iii) According to $f(x, y)$ and $\Phi(x, y)$, a digit can be embedded in any notional system.

The way to find the extraction function coefficient c_B and $\Phi(x, y)$ can be converted to find the following optimal solution:

Minimize $\sum_{i=0}^{B-1} [(x_i - x)^2 + (y_i - y)^2]$, subject to $f(x_i, y_i) \in \{0, 1, \ldots, B-1\}$, where $f(x_i, y_i) \neq f(x_j, y_j)$, if $i \neq j$ and $0 \le i, j \le B - 1$.

According to the above, c_B and $\Phi(x, y)$ can be calculated with different B-ary. For APPM proposed by Hong [10], c_B corresponding to B-ary is listed in Table 1. Meanwhile, parts of $\Phi(x, y)$ corresponding to B-ary are illustrated in Figure 1.

Compared with DE and EMD method, APPM has the flexibility to choose a better notational system for data embedding to decrease the image distortion. The selection

Input: stego image S.
Output: Secret data.
Step 1: Divide the stego image S into non overlapping pixel pairs (x_i', y_i').
Step 2: Calculate $s_i = f(x_i', y_i') = (x_i' + c_B y_i') \bmod B$, where i represents the i-th pixel pair.
Step 3: Calculate all s_i and convert them to binary stream m.

Algorithm 2

(a) Lena (b) Barbara (c) Pepper (d) Boat

(e) Tiffany (f) Baboon (g) Zelda (h) Airplane

Figure 3: The eight gray cover images.

(a) Lena (b) Barbara (c) Pepper (d) Boat

(e) Tiffany (f) Baboon (g) Zelda (h) Airplane

Figure 4: The eight stego images (B=27, PSNR=45dB).

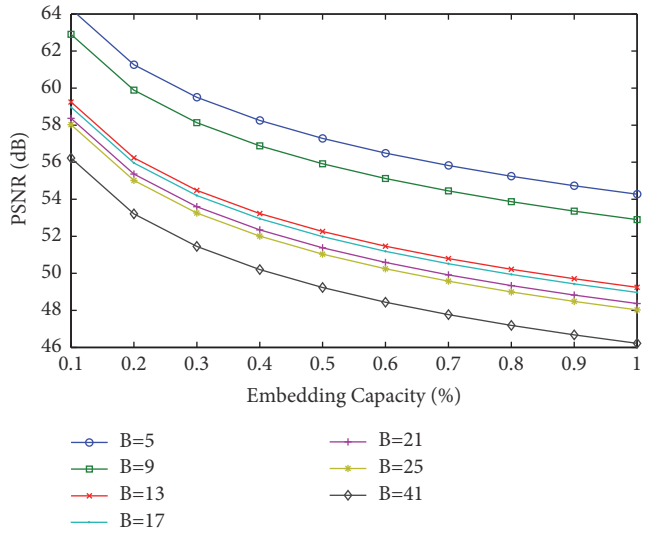


Figure 5: The relationships between embedding payload and image quality.

of B-ary system is determined by the size of the cover image C. Given the size of C is $M \times N$, B is the minimum value satisfying $\lfloor M \times N/2 \rfloor \geq |s_B|$. However, it needed to calculate, store, and query the neighborhood set as shown in Figure 1.

3. The Proposed Formula Adaptive Pixel Pair Matching Method (FAPPM)

In order to solve the above shortcomings, this paper puts forward a formula adaptive pixel pair matching embedding method to find the stego-pixel pair without a neighborhood set.

3.1. Embedding Procedure. In the embedding procedure, four vectors at most are produced. Two vectors are calculated when $D>0$, and the other two vectors are calculated when $D<0$. In Algorithm 1, i represents vectors 1 to 4 in turn. Figure 2 shows the embedding process overview.

Example 1. For a cover pixels pair $(5, 6)$, secret data $s = 8_{(16)}$, and extraction function coefficient $c_{16} = 6$, the stego image pixels pair $(x_1', x_2') = (4, 6)$ is obtained by using Algorithm 1.

Step 1. Calculate $f = (5 + 6 \times 6) \bmod 16 = 9$, $k = \lceil (\lceil \sqrt{B} \rceil - 1)/2 \rceil = 2$.

Step 2. Calculate $D = s - f = -1$. As $D < 0$, $D = D + B = 15$ is obtained.

Step 3. Calculate $next\_t_1 = |D| \bmod c_{16} = 3$.

(1) Round 1: $t_1 = 3, t_2 = 2$.

(2) $|t_1| > k \&\& |t_2| > k$, then $next\_t_1 = t_1 - c_B = -3$.

(3) Round 2: $t_1 = -3, t_2 = 3$.

(4) $|t_1| > k \&\& |t_2| > k$, then $D = D - B = -1, next\_t_1 = -(|D| \bmod c_{16}) = -1$.

(5) Round 3: $t_1 = -1, t_2 = 0$.

(6) $|t_1| \leq k \&\& |t_2| \leq k$, then return $(4, 6)$.

3.2. Extraction Procedure. Through extraction function, secret digits can be extracted from the stego image. The detailed process is given in Algorithm 2.

3.3. Overflow Problem and Solution. If an overflow or underflow problem occurs, that is, $(x', y') < 0$ or $(x', y') > 255$, a nearest (x'', y'') should be found in the neighborhood of (x, y) such that $f(x'', y'') = s_B$. This can be done by solving the optimization problem

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

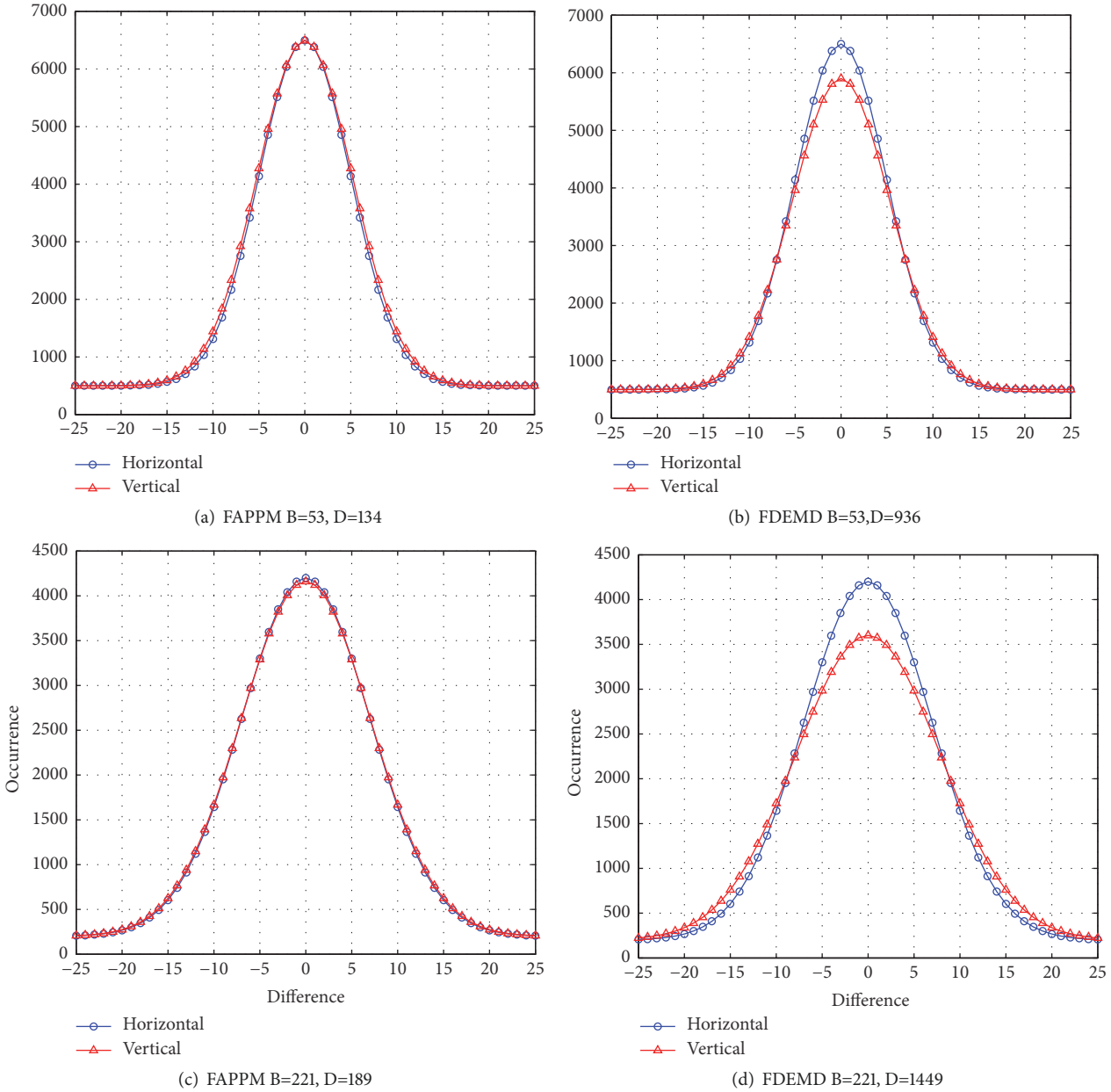
4. Experimental Results and Analysis

4.1. Experimental Results. The experiments are performed using Matlab R2013a, and eight 512×512 grayscale images are used as shown in Figure 3. The stego images are shown in Figure 4, where B=27.

As seen from Figures 3 and 4, the difference between the cover images and the corresponding stego images is very little and can not be distinguished by human's eyes. It illustrated the good imperceptibility of the proposed method.

As message embedding, it will introduce the distortion in the image. Peak signal-to-noise ratio (PSNR) is usually used to measure the quality of image. The definition of PSNR is as follows:

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



(a) FAPPM B=53, D=134

(b) FDEMD B=53,D=936

(c) FAPPM B=221, D=189

(d) FDEMD B=221, D=1449

Figure 6: Comparison of the averaged vertical and horizontal difference histograms of FAPPM and FDEMD.

where MSE is the mean square error between the cover image and stego image; it is defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=0}^{N} \left(p_{i,j} - p'_{i,j} \right)^2 \quad (4)$$

Here, the symbols $p_{i,j}$ and $p'_{i,j}$ represent the pixel values of the cover image and stego image in the position (i, j), respectively, and M and N are the width and height of the original image.

As the proposed method can embed secret digit in any notional system, experiments are done to test the relationship between embedding payload and image quality, and the results are shown in Figure 5. It can be found that the PSNR is decreased as the embedding capacity is increased. However, the PSNR still achieved a high value when the embedding capacity reached 1%.

4.2. Comparison with Other Methods. Here EMD [8], EMD-3 [9], APPM, and FAPPM are compared from six aspects: the embedding method, the national system, payload, capacity, PSNR, and the storage space. The results are listed in Table 2. As seen from Table 2, FAPPM method uses a mathematical method to embed secret data and it does not need any space to store neighbor table; furthermore, it does not affect the capacity and image quality.

Table 2: Comparison of results.

Contents of comparison	EMD[8]	EMD-3[9]	APPM[10]	Proposed FAPPM
Embedding method	Matrix and search	Matrix and search	table look-up	Mathematic method
Notational systems of B-ary	fixed	fixed	arbitrary	arbitrary
Payload (bpp) B=25	2.471	2.471	2.32	2.32
PSNR (dB)	43.9	42.9	48.1	48.1
Need the storage space	Yes	Yes	Yes	No

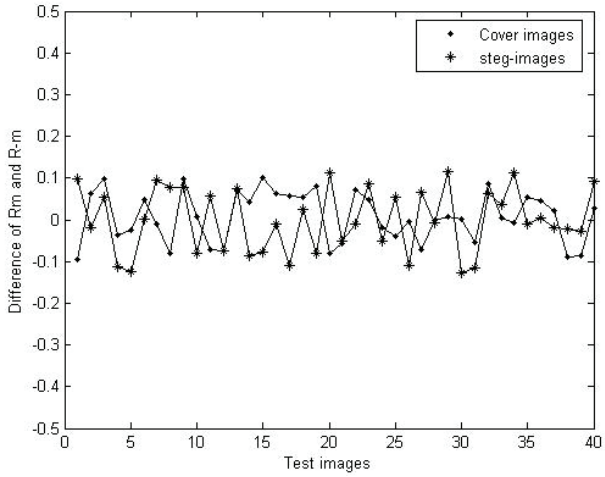


Figure 7: The difference of *Rm* and *R-m* for RS attack.

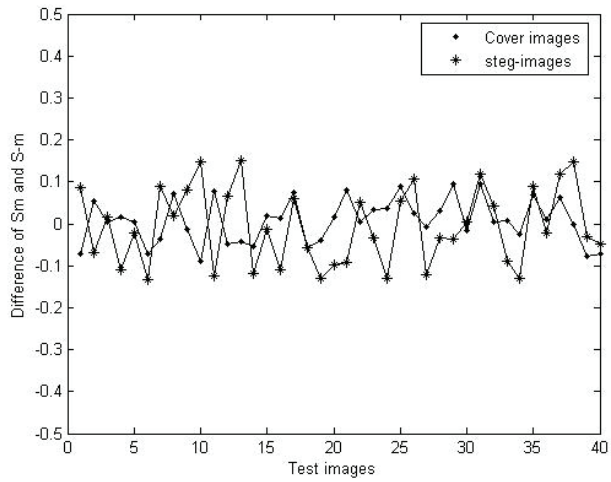


Figure 8: The difference of *Sm* and *S-m* for RS attack.

4.3. Analysis of the Security. Anti-steganalysis is one of the most important criteria to measure the performance of a steganographic method. In this paper, a detection method based on histogram differential statistics analysis proposed by Zhao [18] is used to test the security of the FAPPM method. Normally, in an image with no hiding message, the horizontal difference histogram $\widehat{H}_h$ and the vertical difference histogram $\widehat{H}_v$ are coincident. But, when the message is embedded in a pair of pixels, its $\widehat{H}_h$ and $\widehat{H}_v$ will be changed. The distance between $\widehat{H}_h$ and $\widehat{H}_v$ is used to construct a statistical detector to detect the variation between histograms. The distance is defined as follows:

$$D = \left(\sum_{i=-2T}^{2T} \left(\widehat{H}_h(i) - \widehat{H}_v(i) \right) \right)^{1/2} \quad (5)$$

where T is a predefined threshold and D represents the difference between $\widehat{H}_h$ and $\widehat{H}_v$. The larger the D is, the greater the difference between $\widehat{H}_h$ and $\widehat{H}_v$ is. That is, the probability that the image contains secret information is high. Here experiments are done to compare the histogram variation of FAPPM and FDEMD under high payload. Both FAPPM and FDEMD methods are used to generate 100 stego images, respectively. $\widehat{H}_h$, $\widehat{H}_v$, and their average value are calculated, respectively. The parameters are B=53, B=211, and T=20. All the test images were fully embedded. The experiment results are shown in Figure 6. It can be seen that there is almost no difference between $\widehat{H}_h$ and $\widehat{H}_v$ for FAPPM, while that for FDEMD is significant, which indicates the probability that the successful steganalysis for FDEMD is higher than that of the proposed method.

The RS attack method can detect LSB secret data embedding in grayscale or color images. Each pixel block is classified into the regular group R, the singular group S, and the unusable group U by a flipping function and mask M. *Rm*, *Sm*, and *Um* denote the number of R, S, and U, respectively. For inverse mask *-M*, *R-m, S-m, and U-m* denote the number of R, S, and U, respectively. When no information is embedded, *Rm -R-m*≈0 and *Sm -S-m*≈0. The RS attack results are shown in Figures 7 and 8. It can be seen that the algorithm of this paper can guarantee *Rm -R-m*≈0 and *Sm -S-m*≈0, and the existence of secret information cannot be detected by RS steganalysis method.

5. Conclusion

This paper proposed a simple and convenient data embedding method based on APPM. Compared with the APPM method, it has the advantage of no needing to compute and store the neighborhood set. Compared with the FDEMD method, the secret data of any notional system is realized by the FAPPM method, which makes the embedding notational system selection more flexible. The experimental results showed that FAPPM method has high image quality and the strong anti-steganalysis ability. Our future work will be concentrated on the use of the formula method of the adjacent three pixels as the embedding unit.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by project supported by National Natural Science Foundation of China (Grant no. 61572182, no. 61370225) and project supported by Hunan Provincial Natural Science Foundation of China (Grant no. 15JJ2007).

References

[1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge University Press, New York, NY, USA, 2009.

[2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[3] M. Hussain, A. W. Wahab, Y. I. Idris, A. T. Ho, and K. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.

[4] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003.

[5] J. Fridrich, M. Goljan, and R. Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images," *The Workshop on Multimedia & Security: New Challenges ACM*, pp. 22–28, 2002.

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

[7] 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.

[8] C. Kim, "Data hiding by an improved exploiting modification direction," *Multimedia Tools and Applications*, vol. 69, no. 3, pp. 569–584, 2014.

[9] X. Niu, M. Ma, R. Tang, and Z. Yin, "Image steganography via fully exploiting modification direction," *International Journal of Security and Its Applications*, vol. 9, no. 5, pp. 243–254, 2015.

[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, no. 1, pp. 176–184, 2012.

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

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

[13] R. Chao, H. Wu, C. Lee, and Y. Chu, "A Novel Image Data Hiding Scheme with Diamond Encoding," *EURASIP Journal on Information Security*, vol. 2009, no. 1, p. 658047, 2009.

[14] W.-C. Kuo, P.-Y. Lai, C.-C. Wang, and L.-C. Wuu, "A formula diamond encoding data hiding scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 6, pp. 1167–1176, 2015.

[15] W. Hong, M. Chen, T. Chen, and C. Huang, "An efficient authentication method for AMBTC compressed images using adaptive pixel pair matching," *Multimedia Tools & Applications*, vol. 77, no. 4, pp. 4677–4695, 2018.

[16] T. Edwina Alias, D. Mathew, and A. Thomas, "Steganographic Technique Using Secure Adaptive Pixel Pair Matching for Embedding Multiple Data Types in Images," in *Proceedings of the 5th International Conference on Advances in Computing and Communications, ICACC 2015*, pp. 426–429, India, September 2015.

[17] J. Pappachan and J. Baby, "Transformed adaptive pixel pair matching technique for colour images," in *Proceedings of the International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT 2015*, pp. 192–196, India, December 2015.

[18] H. Zhao, H. Wang, and M. Khurram Khan, "Statistical analysis of several reversible data hiding algorithms," *Multimedia Tools and Applications*, vol. 52, no. 2-3, pp. 277–290, 2011.