


Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm

Fangjun Huang() , Yane Zhong, and Jiwu Huang

School of Information Science and Technology,
Sun Yat-Sen University, Guangzhou 510006, China
huangfj@mail.sysu.edu.cn

Abstract. In edge adaptive image steganography based on LSB matching revisited algorithm (EAMR for short in this paper), the secret message bits are embedded into those consecutive pixel pairs whose absolute difference of grey values are larger than or equal to a threshold T . Tan *et al.* [1] pointed out that since those adjacent pixel pairs can be located by the potential attackers, the pulse distortion introduced in the histogram of absolute difference of pixel pairs (HADPP for short in this paper) can easily be discovered, and a targeted steganalyzer for revealing this pulse distortion is presented in [1]. In this paper, we propose an improved algorithm for EAMR, in which the adjacent pixel pairs for data hiding are selected in a new random way. Thus the attackers cannot locate the pixel pairs selected for data hiding accurately, and the abnormality that exists in HADPP cannot be discovered any longer. Experimental results demonstrate that our improved EAMR (I-EAMR) can efficiently defeat the targeted steganalyzer presented by Tan *et al.* [1]. Furthermore, it can still preserve the statistics of the carrier image well enough to resist today's blind steganalyzers.

Keywords: Pixel pairs · Histogram · Steganography · Steganalyzer

1 Introduction

Digital image steganography is a new approach to transmit the secret message without arousing the suspicion of potential attackers. In spatial domain image steganography, the secret message bits are usually embedded into image by modifying the pixel values.

Least significant bit (LSB) replacement is a well-known steganography method. In this embedding scheme, if the secret bit is equal to the LSB of the pixel value, the pixel does not need to be modified. Otherwise only the LSB of the pixel is overwritten with the secret bit. Since LSB replacement modifies only the LSBs of the pixels in the image, the pairs of values (PoVs) [2] will be generated in the stego image. Thus it is very easy to detect the existence

of the hidden message even at a low embedding rate using some reported steganalytic algorithms, such as Chi-squared [2], regular groups (RS) analysis [3]. LSB matching (LSBM) is a counterpart of LSB replacement. In the embedding process, LSB matching does not simply overwrite the LSBs of the cover pixels. Instead, the value of the cover pixel is randomly increased or decreased by 1 if its LSB does not match the secret message bit to be embedded, and thus PoVs will not exist in the stego image. Therefore, the traditional methods used to detect LSB replacement cannot attack LSBM successfully.

In 2006, Mielikainen proposed LSB matching revisited (LSBMR) steganography [4]. Unlike LSB replacement and LSBM, which deal with the pixels independently, LSBMR considers a pair of pixels (p_i, p_{i+1}) as an embedding unit. This new scheme can reduce the expected number of modifications per message bit embedding from 0.5 to 0.375 compared with LSB replacement and LSBM. Thus LSBMR introduces less distortion to the carrier image and will be more difficult to be detected compared with LSBM approach. However, Tan [5] pointed out that LSBMR and its descendants would introduce intrinsic imbalance in data hiding process which might result in the imbalance of the power of the additive stego noise, and put forward a targeted steganalysis against LSBMR using B-Spline function [16].

However, the typical LSB-based approaches, such as LSB replacement, LSBM and LSBMR, embed the message into the cover image randomly without considering the statistics of the cover image. In [6], Luo *et al.* pointed out that the statistical characteristics of the edge regions are more complicated than that of the flat regions and will be preserved much better after data hiding. They proposed a new adaptive steganography called edge adaptive image steganography based on LSB matching revisited (EAMR) [6], and received much attention [1, 17]. In this new algorithm, the absolute difference value between two consecutive pixels was utilized for selecting the embedding regions. The experiments demonstrated that EAMR can resist today's blind steganalyzers efficiently, such as Shi-78D [7], Farid-72D [8], Moulin-156D [9] and Li-110D [10]. However, this new method still has some limitations. Tan *et al.* [1] pointed that EAMR introduced a pulse distortion to the long exponential tail in HADPP, and they proposed a targeted steganalytic scheme based on B-Spline fitting [11]. The experimental results demonstrated that the proposed method could detect EAMR efficiently even if the embedding rate was as low as 0.05 bits per pixel (bpp).

In this paper, we propose an improved algorithm for EAMR. Different from that in EAMR the consecutive pixel pairs are generated based on raster scanning. In our algorithm, the carrier image will be divided into 3×3 non-overlapping blocks, and the adjacent pixel pairs are randomly selected from each 3×3 block according to different directions. Thus the selected pixel pairs cannot be located by the potential attackers and the pulse distortion introduced in HADPP cannot be discovered any longer. Experimental results demonstrate that our improved EAMR (I-EAMR) can not only efficiently defeat the targeted steganalyzer presented by Tan *et al.* [1], but can also resist today's blind steganalyzers successfully.

The rest of this paper is organized as follows. In Sect. 2, some previous works about EAMR are briefly reviewed. Our improved algorithm of EAMR is introduced in Sect. 3. Experimental results are illustrated in Sect. 4 and the conclusions are made in Sect. 5.

2 Previous Works

2.1 Overview of EAMR

EAMR [6] is a content-adaptive scheme based on LSBMR scheme. The absolute difference values between two consecutive pixels are utilized for selecting the embedding regions. For example, if the absolute difference value is bigger than a predetermined threshold T , this pair of pixels can be selected for data hiding. Otherwise, this pair of pixels cannot be selected for data hiding. The embedding procedures are described as follows.

Step1: The cover image is first divided into non-overlapping blocks with the size of $B_Z \times B_Z$ (where $B_Z \in \{1, 4, 8, 16\}$). Each block is randomly rotated 0, 90, 180, 270 degrees. The resulted image is rearranged as a row vector via raster scanning. Then the vector is divided into non-overlapping embedding units with every two consecutive pixels (p_i, p_{i+1}) . Let S be the set of consecutive pixel pairs.

Step2: For a given secret message M , the threshold T for region selection can be determined by Eq. (2). Let $EU(t)$ be the set of pixel pairs whose absolute difference values are larger or equal to a parameter t .

$$EU(t) = \{(p_i, p_{i+1}) | |p_i - p_{i+1}| \geq t, \forall (p_i, p_{i+1}) \in S\} \quad (1)$$

The threshold T can be calculated by

$$T = \arg \max_t \{2 \times |EU(t)| \geq |M|\} \quad (2)$$

where $t \in \{0, 1, \dots, 31\}$, $|EU(t)|$ is the total number of pixel pairs in $EU(t)$, and $|M|$ is the length of the secret message M .

Step3: For each pixel pair (p_i, p_{i+1}) in $EU(T)$, the LSBMR algorithm is conducted. Let (p'_i, p'_{i+1}) be the corresponding output of (p_i, p_{i+1}) after embedding, and (m_i, m_{i+1}) be the two secret bits to be embedded. Note that after embedding, the new difference $|p'_i - p'_{i+1}|$ may be less than the predetermined threshold T . Thus a readjusting strategy should be used to guarantee that the absolute difference values between the two modified pixels are still no less than T . In addition, if the modified pixels p'_i or p'_{i+1} is out of the range $[0, 255]$, the readjusting strategy should also be utilized to ensure that the modified pixels are still in the range of $[0, 255]$. Otherwise, the receiver cannot locate the pixel pair utilized for data hiding and the embedded message cannot be extracted successfully. Assume that (p_i, p_{i+1}) is readjusted to (p''_i, p''_{i+1}) . The readjusting scheme is as follows

$$(p_i'', p_{i+1}'') = \arg \min_{(e_1, e_2)} \{|e_1 - p_i| + |e_2 - p_{i+1}|\} \quad (3)$$

where $e_1 = p_i' + 4k_1$, $e_2 = p_{i+1}' + 2k_2$, $|e_1 - e_2| \geq T$, $0 \leq e_1, e_2 \leq 255$, $k_1, k_2 \in \mathbf{Z}$. Please refer to the appendix in [6] for more details about the readjusting strategies.

2.2 Tan *et al.*'s Targeted Steganalysis of EAMR

In [1], Tan *et al.* pointed out that the readjusting procedure of EAMR introduced a distortion to the long exponential tail of the HADPP. Generally, the HADPP of a natural cover image usually rises to a peak at a small gradient value, and then falls off but still has a very long exponential tail [12]. However, the HADPP of EAMR stego images violates the above-mentioned law. In [1], Tan *et al.* have proved that the readjusting procedure of EAMR made the numbers of pixel pairs whose absolute difference values were equal to $T+1$ would be larger than the number of pixel pairs whose absolute difference values were equal to T in the HADPP.

One image is randomly selected from BOWS-2 [13] for an illustration, which is shown in Fig. 1. The corresponding pulse distortion introduced by the EAMR readjusting procedure is shown in Fig. 2. Figure 2(a) shows an HADPP (the difference values in the range of [10, 35] are illustrated) of the cover image illustrated in Fig. 1. As seen, in the cover image the frequencies of pixel pairs in different gradient values decrease quickly but smoothly with the increasing of the difference values. Figure 2(b) is the corresponding HADPP of the stego image generated using EAMR algorithm with the embedding rate of 0.1 bpp, where the predetermined threshold T is selected as 31. Comparing Fig. 2(a) and Fig. 2(b), we can find out that a pulse distortion around $T = 31$ in the HADPP (The area inside the circle in Fig. 2(b)).

Tan *et al.* have constructed a targeted steganalyzer based on B-Spline fitting [11] for detecting this pulse distortion. The method of Tan *et al.*'s targeted steganalyzer of EAMR is as follows. Firstly, two sets of consecutive pixel pairs are



Fig. 1. A cover image randomly selected from BOWS-2 [13].

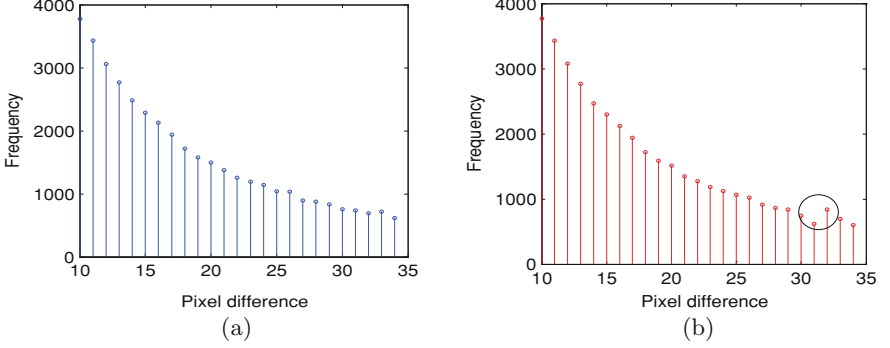


Fig. 2. (a) The HADPP of Fig. 1 with difference values being in the range of $[10, 35]$. (b) The corresponding HADPP of EAMR stego image with the embedding rate of 0.10 bpp and $T = 31$.

created: V_S of the test image and V_R of the rotated image (i.e., non-overlapping blocks with the size of $B_Z \times B_Z$ in the test image are rotated for 90 degrees). Secondly, the HADPPs for V_S and V_R are generated. Then the fitting-error ε_i is computed by Eq. (4)

$$\varepsilon_i = b_i - g(t_i), i = 0, 1, \dots, 36 - k (t_0 = 0, t_n = 1, t_{i+1} - t_i = \frac{1}{n}) \quad (4)$$

where $b_i, i = 0, 1, \dots, 36 - k, b_i \in \mathbf{N}$ is a sequence of bin values in HADPP with the difference values being in the range of $[k, 36]$ (k is used to omit the unwanted peak in the HADPP and is set to 3 in Tan *et al.*'s work [1]), and $g(t_i)$ be a fitting spline of the HADPP. The function f is defined as $f = \varepsilon_{i+1} - \varepsilon_i$ ($i = 0, 1, \dots, 32$), and the maximum value of function f is used as the feature to discriminate the presence of EAMR steganography. Assume the corresponding feature of V_S and V_R are D_S and D_R . The targeted image is judged as a stego image if D_S or D_R is larger than a predetermined threshold θ . Their experimental results demonstrated that EAMR algorithm could be detected accurately even though the embedding rate is as low as 0.05 bpp.

3 Improved EAMR

3.1 Generation of the Set of Adjacent Pixel Pairs

As seen, EAMR method embeds secret bits into consecutive pixel pairs which are created by raster scanning. Those consecutive pixel pairs may be located accurately and the pulse distortion introduced in the HADPP can be discovered.

In our improved scheme, we propose a new method to generate a random set of pixel pairs for data hiding, which are not constructed according to the raster scanning as that in EAMR. Thus the potential attackers cannot locate

the adjacent pixel pairs accurately and the security performance of EAMR can be improved. In our proposed method, the generation of the set of pixel pairs is controlled by a secret key. These two pixels can be selected from a 3×3 block according to different directions, such as horizontal, vertical, 45 degrees or 135 degrees, as shown in Fig. 3. There are 6 kinds of strategies to select pixel pairs in a 3×3 block, which are shown in Fig. 4, where each double arrow indicates a pair of adjacent pixel pairs. The specific steps for generating a random set of pixel pairs are as follows:

Step1: The image with the size of $m \times n$ is divided into 3×3 non-overlapping blocks, and the number of blocks is $N = \text{floor}(m/3) * \text{floor}(n/3)$. Then a random number sequence $\{B_1, B_2, \dots, B_N\}$ is generated, which is controlled by a secret key k_1 .

Step2: For any random number B_i , compute $B_i \% 6$. If the remainder is j , we choose the $j+1$ th strategy to select the adjacent pixel pairs. Note that in Fig. 4 there are 6 strategies for selecting the pixel pairs and each sub-figure represents one selecting strategy, respectively. The obtained adjacent pixel pairs will be added to a predetermined pixel pair set S . For example, assuming $B_i = 200$ and $B_i \% 6 = 2$, the strategy described in Fig. 4(c) will be selected to generate pixel pairs. As a result, the pixel pairs put in set S are $(p_{x-1,y-1}, p_{x,y-1})$, $(p_{x-1,y}, p_{x-1,y+1})$, $(p_{x,y}, p_{x+1,y+1})$ and $(p_{x,y+1}, p_{x+1,y})$, where $p_{x,y}$ represents the pixel in the center of the 3×3 block of Fig. 4(c).

Step3: Repeat Step2 until all non-overlapping 3×3 blocks are visited and all the pixel pairs are added into the set S .

3.2 Our Improvement on EAMR

In this section, we will introduce our Improved EAMR algorithm (I-EAMR for short). The detailed procedures are as follows.

Step1: The cover image A with the size of $m \times n$ is divided into $B_Z \times B_Z$ non-overlapping blocks (where $B_Z \in \{1, 4, 8, 16\}$). Each block is randomly rotated 0, 90, 180, 270 degrees and then gets the rotated image A' . This step is the same as that in EAMR algorithm.

Step2: Apply our proposed method for generating the set of adjacent pixel pairs to A' and get a pixel pairs set S , as described in Sect. 3.1.

Step3: The following steps are the same as Step 2–3 of EAMR algorithm as described in Sect. 2.1.

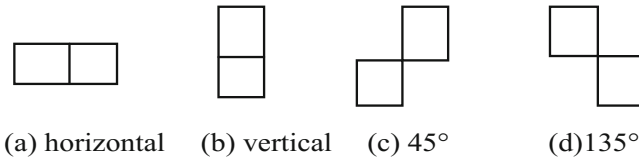


Fig. 3. Four embedding directions.

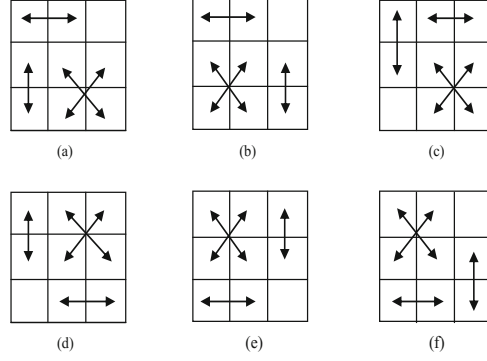


Fig. 4. The 6 kinds of different strategies for selecting the pixel pairs in a block.

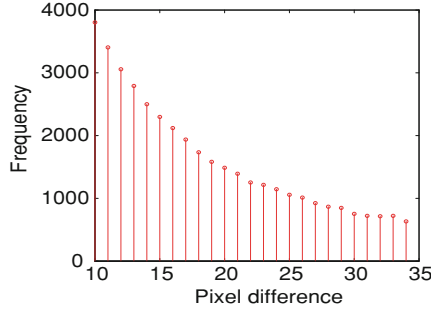


Fig. 5. The HADPP of I-EAMR stego image generated from the cover image Fig. 1 ($T = 31$ which is corresponding to 10% embedding rate) in the range of [10, 35].

As seen, in I-EAMR algorithm, the strategy to embed secret message into cover elements is almost the same as that in EAMR except that the strategy for generating the adjacent pixel pairs is different. However, via using new generating strategy, the potential attackers may not locate the pixel pairs for data hiding accurately, thus the pulse distortion existing in the HADPP cannot be discovered any longer and the security performance of EAMR will be improved greatly. Figure 5 illustrates the corresponding HADPP of the stego image generated using our I-EAMR algorithm. The image illustrated in Fig. 1 is selected as the cover image and the embedding rate is 0.10 bpp. It is observed from Fig. 5 that the HADPP of the I-EAMR stego image is almost the same as that of the cover image. Thus the targeted steganalyzer presented by Tan *et al.* [1] will not be able to detect the existence of secret message in the I-EAMR stego images any longer.

4 Experimental Results

In this section, some experimental results will be given to demonstrate the effectiveness of our proposed I-EAMR algorithm. The testing image database in our experiments is BOWS-2 [13], which consists of 10,000 grayscale images with a size of 512×512 .

One targeted steganalyzer and three kinds of blind steganalyzer are selected in our testing. The targeted steganalyzer is Tan *et al.*'s method with 2 dimensional features [1] (Tan-2D for short in this paper). The three blind steganalyzers are Shi-78D [7], Li-110D [10], and SPAM-686D [14], respectively, where

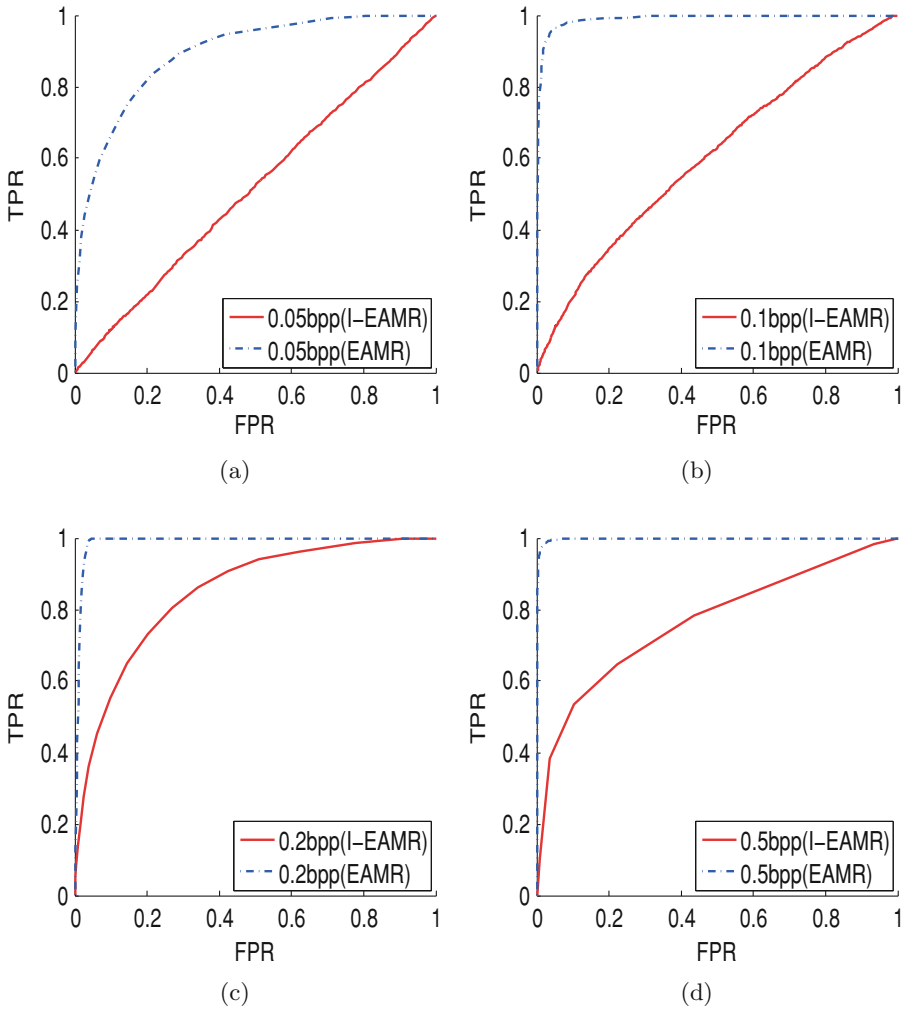


Fig. 6. ROC curves of Tan-2D steganalyzer while detecting I-EAMR and EAMR algorithms with different embedding rates.

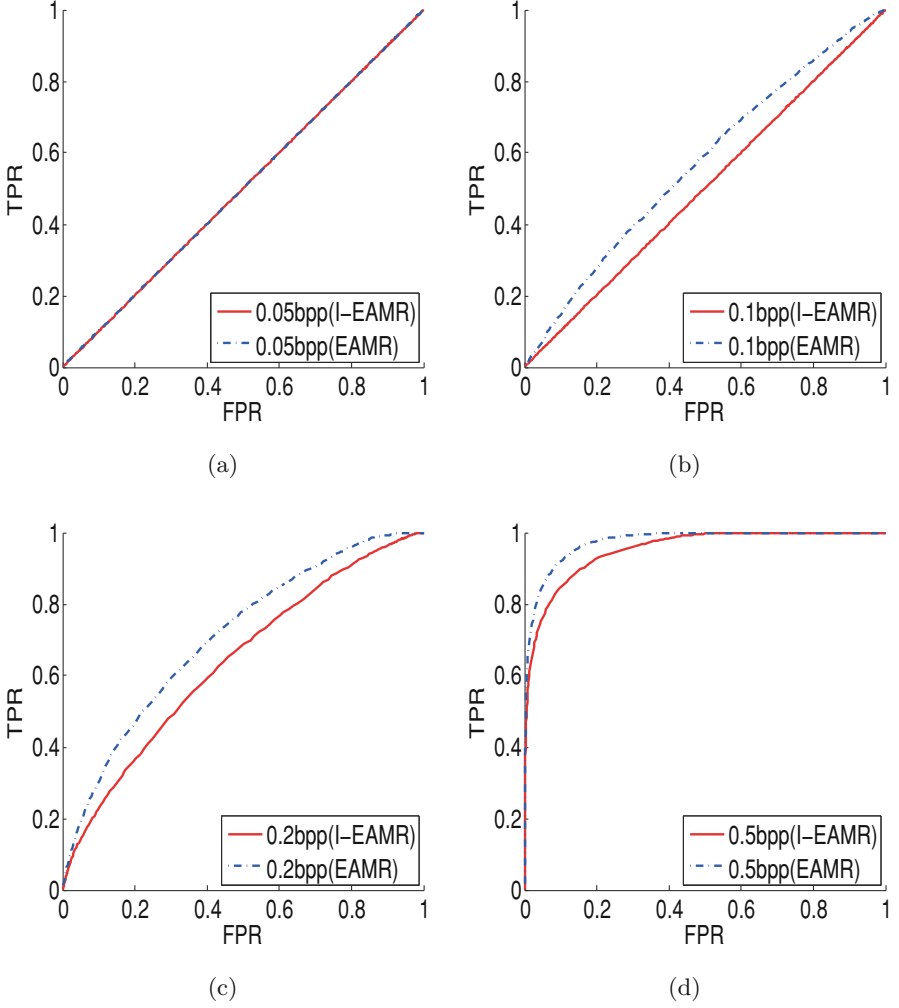


Fig. 7. ROC curves of Shi-78D while detecting I-EAMR and EAMR algorithms with different embedding rates.

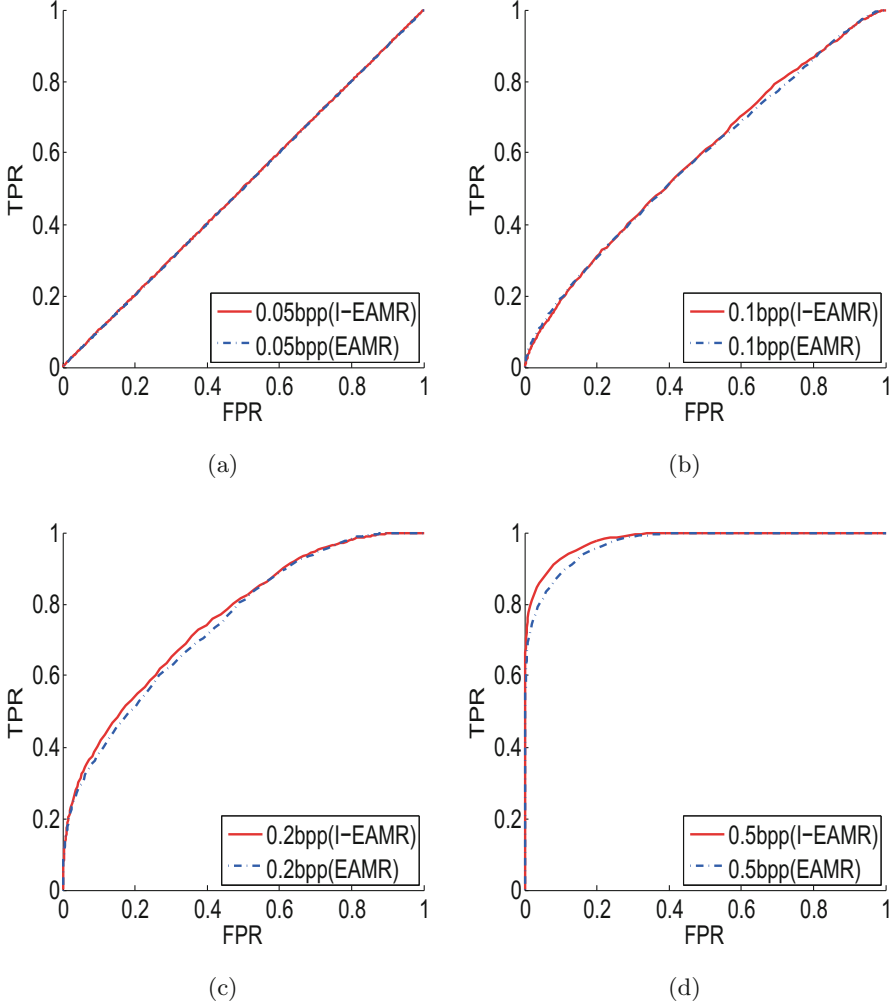


Fig. 8. ROC curves of Li-110D while detecting I-EAMR and EAMR algorithms with different embedding rates.

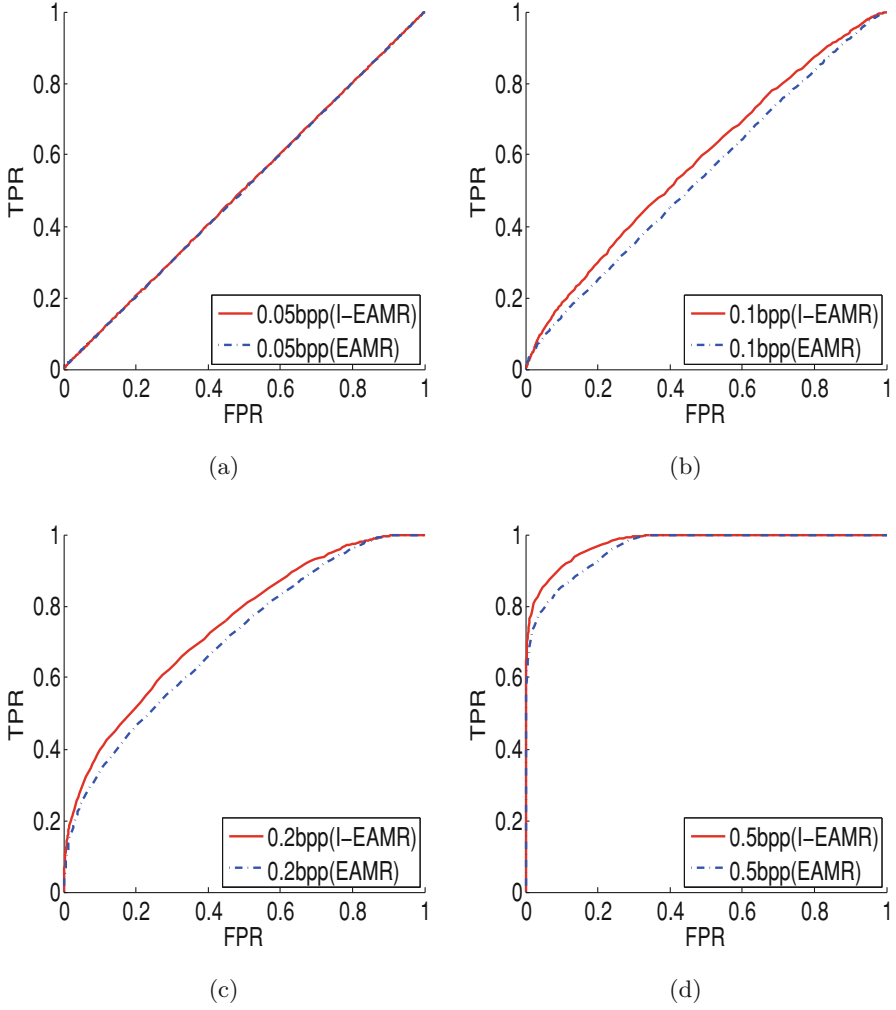


Fig. 9. ROC curves of SPAM-686D while detecting I-EAMR and EAMR algorithms with different embedding rates.

Shi-78D [7] and Li-110D [10] are two of the most efficient steganalyzers used for detecting EAMR in [6]. To the best of our knowledge, the SPAM-686D is one of the most efficient universal steganalyzers for detecting today's spatial domain steganography.

In order to demonstrate the security performance of our improved algorithm, EAMR has also been conducted in our testing for a comparison. The stego images are generated using I-EAMR and EAMR algorithm with the embedding rates of 0.05, 0.1, 0.2, 0.5 bpp, respectively. In our testing, 5,000 randomly selected cover images and their corresponding stego counters are used for training and the remaining cover and stego images are used for testing. We adopt LIBSVM [15] for training and testing in all experiments. In Figs. 6, 7, 8 and 9, the Receiver Operating Characteristic (ROC) curves corresponding to different steganalyzers (i.e., Tan-2D, Shi-78D, Li-110D and SPAM-686D) are illustrated.

It is observed from Fig. 6 that our new algorithm is efficient in defeating the targeted steganalyzer Tan-2D. As seen, when the embedding rate is about 0.05 bpp, EAMR can easily be detected by Tan-2D. However, when the embedding rate is increased to 0.10 bpp, the final detection accuracy rates of I-EAMR is still around random guessing. Even if the embedding rate is increased to 0.15 bpp or 0.20 bpp, the security performance of I-EAMR is still much better than EAMR in general. Note that in our experiments, in order to get the best possible detection performance, the parameter k (described in Sect. 2.2) of Tan-2D used to omit the unwanted peak in the HADPP is set to 4 in Fig. 6(a-c), and the parameter k is set to 3 in Fig. 6(d).

It is observed from Figs. 7, 8 and 9 that I-EAMR and EAMR may have the same security performance when Shi-78D, Li-110D and SPAM-686D are selected as the steganalyzers. That is, the improvement made on EAMR will not decrease the resisting capability of EAMR against the blind steganalyzers.

5 Conclusions

In this paper, we have proposed an Improved EAMR algorithm (I-EAMR) to resist the targeted steganalyzer proposed by Tan *et al.* [1]. Via a new strategy for generating adjacent pixel pairs, the potential attackers cannot locate the embedding pixel pairs accurately, and thus the abnormality existing in the absolute difference histogram cannot be detected. Experimental results demonstrate that our improved algorithm I-EAMR can not only resist the targeted steganalyzer proposed by Tan *et al.*, but also has the capability for resisting today's most powerful blind steganalyzers.

Acknowledgments. The authors would like to thank Dr. Shunquan Tan at Shenzhen University, Shenzhen, China, for providing us the source code in [1]. This work was supported by the National Natural Science Foundation of China (61173147, U1135001), the 973 Program of China (2011CB302204), the Key Projects in the National Science & Technology Pillar Program (2012BAK16B06), the Fundamental Research Funds for

Central Universities (12lgpy31), and the Project Sponsored by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry ([2012]1707).

References

1. Tan, S., Li, B.: Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-spline fitting. *IEEE Sig. Process. Lett.* **19**(6), 336–339 (2012)
2. Westfeld, A., Pfitzmann, A.: Attacks on steganographic systems. In: Pfitzmann, A. (ed.) *IH 1999. LNCS*, vol. 1768, pp. 61–76. Springer, Heidelberg (2000)
3. Fridrich, J., Goljan, M., Du, R.: Detecting LSB steganography in color, and gray-scale images. *IEEE Multimedia* **8**(4), 22–28 (2001)
4. Mielikaieen, J.: LSB matching revisited. *IEEE Sig. Process. Lett.* **13**(5), 285–287 (2006)
5. Tan, S.: Steganalysis of LSB matching revisited for consecutive pixels using B-spline functions. In: Shi, Y.Q., Kim, H.-J., Perez-Gonzalez, F. (eds.) *IWDW 2011. LNCS*, vol. 7128, pp. 16–29. Springer, Heidelberg (2012)
6. Luo, W., Huang, F., Huang, J.: Edge adaptive image steganography based on LSB matching revisited. *IEEE Trans. Inf. Forensics Secur.* **5**(2), 201–214 (2010)
7. Shi, Y.Q., et al.: Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network. In: *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 269–272 (2005)
8. Farid, H.: Detecting hidden messages using higher-order statistical models. In: *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, pp. 905–908 (2002)
9. Wang, Y., Moulin, P.: Optimized feature extraction for learning-based image steganalysis. *IEEE Trans. Inf. Forensics Secur.* **2**(1), 31–45 (2007)
10. Li, B., Huang, J., Shi Y.Q.: Textural features based universal steganalysis. In: *Proceedings of the Spie on Security, Forensics, Steganography and Watermarking of Multimedia*, vol. 6819, p. 681912 (2008)
11. Unser, M.: B-spline signal processing: part I-theory. *IEEE Trans. Signal Process.* **41**(2), 821–833 (1993)
12. Ruderman, D.L.: The statistics of natural images. *Netw.: Comput. Neural Syst.* **5**, 517–548 (1994)
13. Bas, P., Furon, T.: BOWS-2, July 2007. <http://bows2.gipsa-lab.inpg.fr>
14. Pevny, T., Bas, P., Fridrich, J.: Steganalysis by subtractive pixel adjacency matrix. *IEEE Trans. Inf. Forensics Secur.* **5**(2), 215–224 (2010)
15. Chang, C.C., Lin, C.J.: LIBSVM : a library for support vector machines. *ACM Trans. Intell. Syst. Technol.* **2**(27), 1–27 (2011)
16. Wahba, G.: Smoothing noisy data with spline functions. *Numer. Math.* **24**, 383–393 (1975)
17. Li, X., et al.: Steganalysis of a PVD-based content adaptive image steganography. *Sig. Process.* **93**, 2529–2538 (2013)

Digital-Forensics and Watermarking

12th International Workshop, IWDW 2013, Auckland,
New Zealand, October 1-4, 2013. Revised Selected
Papers

Shi, Y.Q.; Kim, H.J.; Pérez-González, F. (Eds.)

2014, XVI, 530 p. 239 illus., Softcover

ISBN: 978-3-662-43885-5