A High Efficient FEMD-Based Data Hiding Algorithm

J N Liu, Q Zhou, Y L Hu and J Y Wei

National Key Laboratory of Science and Technology on Space Microwave, CAST
Xi'an, Shaanxi 710100, China

Email: liujuanni0@126.com

Abstract. This paper proposes a high efficient FEMD-based data hiding method suitable for various complexity images. The method uses FEMD's extraction function to map a cover pixel (8 bits) and a randomizable auxiliary pixel (log₂n+1 bits) into a data of n²-ary notational system, which can significantly improve the data hiding efficiency. When n=2, the embedding efficiency of FEMD is 1/8, and that of our method is 1/5, which is increased by 60% and the image quality of the two methods is almost the same. In other words, our method will have higher image quality when the embedding rate of the two methods is same. When n=4 or 8 and the data embedding efficiency is equal, the PSNR of this method is increased by 1.3 dB or 1.1 dB compared with FEMD. In addition, the auxiliary pixel as a key can improve the security of our data hiding algorithm.

1. Introduction

Data hiding is a useful technology for concealing secret messages into cover media (text, image, audio or video) and then transmitting the stego media via public networks without suspicion. The applications of data hiding include military messages covert transmission, tampered data detection, copyright protection and online voting etc. The pure payload and the stego image’s visual quality are the major concerns to evaluate the performance of data hiding scheme, and we need to take a good effect to balance them, since they are confrontational to each other. An excellent hiding algorithm is to provide large capacity with less visual distortion.

In 2006, Mielikainen [1] proposed an improved LSB matching scheme by using two pixels as a unit to embed secret data. However, the modification directions was exploited incompletely. So Zhang and Wang [2] proposed a novel data hiding scheme that exploited modification directions (EMD). In this scheme, the secret message in a (2n+1)-ary notational system is carried by n cover pixels, and only one pixel value is increased or decreased by 1 at most. Though LSB matching and EMD scheme can provide stego image with better visual quality, the possible maximum payload are 1 and 1.161 bpp respectively. In order to increase the hiding capacity, many schemes [3-8] have been developed to improve the performance of EMD with concerns on the hiding capacity and visual quality. In 2009, Chao et al. [3] proposed an image data hiding scheme using diamond encoding (DE). In this scheme, a pair of cover pixels is applied to calculate the diamond characteristic value, which is then modified to the secret message by adjusting pixel values. In order to prevent the overflow and underflow problems, a large distortion and image noise may be caused due to this adjustment with large parameter k. In 2010, Wang et al. [4] proposed a section-wise EMD method, which combined several pixel groups of the cover image together to indicate adjusting modification directions. This scheme further improves the embedding rate and the visual quality of EMD method. In 2011, Kieu and Chang [5] improved the EMD scheme using...
a new embedding function called fully exploiting modification direction (FEMD), which means eight modification directions can be exploited for embedding secret data and the embedding distortion is restricted into a square of various sizes, thus increasing the data hiding capacity from 1 bpp to 4.5 bpp. In 2013, Kuo [6] presented a square fully exploiting modification directions (SFEMD) scheme in order to quickly embed secret data, while maintain the same payload as that of FEMD. Lately, Shen and Huang [7] combined the pixel value differences (PVD) and FEMD algorithm to propose a more secure information hiding algorithm, which is less detectable by RS detection attack. In 2017, Leng [8] proposed a higher capacity data hiding algorithm by using the regular octagon-shaped shell, and there is no need to convert the secret data into a non-binary notational system.

In order to further improve the performance of data hiding algorithm, we propose a novel FEMD-based data hiding algorithm, which can hide \( n^2 \)-ary notational system secret data \( n \in \mathbb{N}, n \geq 2 \) by using auxiliary pixel to form pixel pairs. Since the bits of the auxiliary pixel is \( \log_2(n+1) \), which is significantly smaller than that of the carrier pixel if the value of \( n \) is small \((n \leq 16)\), thus the embedding rate of our algorithm is higher than that of the FEMD method. And the auxiliary pixel value can be used as a key for secret data extraction by the receiver to ensure the security of the algorithm.

We organize the remainder of this paper as follows: the proposed new FEMD-based data hiding scheme will be introduced in Section 2, and the experimental results will be given in Section 3. Finally, Section 4 will give the concluding remarks.

2. The proposed method
The FEMD scheme increases the modification directions of pixel pair from \( 2n+1 \) to \( n^2 \) to improve the hiding capacity, which providing a simple and effective method for large-capacity information hiding. Based on this, an improved FEMD-based data hiding algorithm by adding auxiliary pixel to compose cover pixel pair is proposed. Each cover image corresponds to an auxiliary pixel, whose value is only known by the authorizer and its number of bits is much smaller than the original cover pixel. This can not only significantly increase the embedding rate of secret data but also improve the security of the algorithm.

2.1. Adding auxiliary pixel
In triangular geometry, adding auxiliary lines can make complex problem simple and clear. Inspired by this idea, auxiliary pixel is added to realize FEMD-based data hiding algorithm, for which the pixel pairs still meet the requirements of extraction function, but the amount of cover data will significantly reduced, and the corresponding secret data embedding rate will increased.

In the FEMD method, the variations of the pixel pair \((x, y)\) after hiding secret data satisfy the following equations:

\[
X = \{\Delta x \in Z | -q \leq \Delta x \leq q\} \tag{1}
\]
\[
Y = \{\Delta y \in Z | -q \leq \Delta y \leq q\} \tag{2}
\]

where \( q = [n/2] \). Assuming that \( y \) in the pixel pair is the added auxiliary pixel, denoted as \( y_0 \), its value after embedding the information can be estimated in advance, that is, \( y_0 = y_0 + \Delta y \), and \( y_0 \) equals to any integer in \([q, 255-q]\) can complete the data hiding process, which means its value does not affect the hiding results. At the receiving end, only the stego pixel \( x' \) and the variation \( \Delta y \) are needed to recover the secret data with the assistant of the key \( y_0 \), that is to say, after adding auxiliary pixel \( y_0 \), the secret data can be extracted only by transmitting \( x' \) and \( \Delta y \). It is not difficult to find the original cover pixels \( x \) and \( y \) are both 8-bit data, and \( \Delta y \) only need to be represented by \( \log_2(n+1) \) bit. Therefore, the bits of cover pixel pairs are reduced from \( 8+8 \) to \( 8+(\log_2(n+1)) \), while the hiding capacity remains unchanged. For example, when \( n=2 \), the FEMD method has a hiding capacity of 1bpp and an embedding rate of \( 2/(8+8)=1/8 \). In our algorithm, the hiding capacity is still 1bpp, but the embedding rate is \( 2/(8+2)=1/5 \), which is 60% higher than the FEMD method; when \( n=16 \), the FEMD method has a hiding capacity of
4bpp and an embedding rate of $8/(8+8)=1/2$, and the hiding capacity of our algorithm is still 4bpp, but the embedded rate is $8/(8+5)=8/13$, which is 23% higher than the previous method.

2.2. Data embedding procedure
The information hiding procedure in this paper are as follows:

1). Convert binary secret data into $n^2$-ary notational system. Each $L$-bit binary data is converted into a $K$-bit $n^2$-ary notational system data, and the relationship between the two is

$$L = \lceil K \log_2 n \rceil$$

(3)

where $n=2^k$, the $k$-bit binary data can be completely represented by a bit of $n^2$-ary notational system data, ie. $K=1$ and $L=k$.

2). Generate auxiliary pixel $y_0$. An arbitrary number in $[q, 255-q]$ is generated as the auxiliary pixel $y_0$ by the random number generator.

3). Compose each cover pixel with auxiliary pixel $y_0$ into a pixel pair $(x, y_0)$ and calculate the extraction function value $f$

$$f(x, y) = \left( (n-1) \times x + n \times y \right) \bmod n^2$$

(4)

4). Compare $f$ with a secret data $s$:

4.1). If $f=s$, the pixel pair $(x, y_0)$ is not changed, otherwise the pixel pair is modified according to step 4.2);

4.2). Traverse the sets $X$ and $Y$ that defined by equations (1)-(2), search for the pixel pairs $(x+\Delta x, y_0 + \Delta y)$ that meet the condition $f(x+\Delta x, y_0 + \Delta y) = s$, and select the one with the smallest variation as the result.

5). If the stege pixel pair $(x', y_0')$ overflows, adjust the cover pixel pair according to equation (5) and then re-embed the secret data.

$$\begin{cases} x = x + 1, x' < 0 \\ y_0 = y_0 + 1, y_0' < 0 \\ x = x - 1, x' > 255 \\ y_0 = y_0 - 1, y_0' > 255 \end{cases}$$

(5)

6). Repeat step 3) to 5) until all secret data are embedded.

7). The stego image and the auxiliary pixel variation table are packaged and sent to the receiving end.

2.3. Data extracting procedure
The extraction method of secret data is very simple, the steps are as follows:

1). Use $y_0$ and the auxiliary pixel variation table to get the stego auxiliary pixel, ie. $y_0' = y_0 + \Delta y$.

2).Compose the stego cover pixel with the stego auxiliary pixel into a pixel pair $(x', y_0')$.

3). For each pixel pair $(x', y_0')$, extract 1 bit $n^2$-ary notational system data according to formula (4).

4). Repeat the above steps until all the data is extracted.

5). Convert the extracted $n^2$-ary notational system data with group of $K$ bits into $L$-bit binary information.

3. Experiment results
In this section, we present several experimental results to demonstrate the good performance of our method. Six standard test images are shown in figure 1, which are used as the cover media. The secret data which generated by a pseudo-random number generator are in binary format. If a high level of security is required, cover image can be pre-processed using a chaotic sequence or some well-known encryption methods [9].
The performance of the proposed data hiding algorithm is measured by using Peak Signal to Noise Ratio (PSNR), hidden capacity $C$ and embedding rate $E$. For an 8-bit digital image of size $H \times W$, the PSNR is defined as follows:

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \text{dB}$$  \hspace{1cm} (6)

where $\text{MSE}$ is the mean square error between the original image and the stego image, and the calculation formula is

$$\text{MSE} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} (x_{ij} - \overline{x}_{ij})^2$$  \hspace{1cm} (7)

here, $x_{ij}$ and $\overline{x}_{ij}$ respectively represents the pixel value of the original image and the stego image at position $(i, j)$.

The embedding rate increase percentage is defined as

$$\alpha = \frac{E_2 - E_1}{E_1} \times 100\%$$  \hspace{1cm} (8)

where $E_1$ represents the embedding rate of the comparison scheme and $E_2$ represents the embedding rate of our scheme.

3.1. Embedding rate comparison

In the FEMD method, the parameter $n$ affects the information hiding capacity and the embedding rate. In this paper, the embedding rate can be further improved by adding auxiliary pixel. Table 1 gives the embedding rate comparison results of the two methods when $n=2^8$. In table 1 $C_1$ and $C_2$ respectively represent the hiding capacity of FEMD method and our method, and $E_1$ and $E_2$ respectively represent the embedding rates of the two methods. As the results shown in table 1, the hiding capacity and embedding rate of the two algorithms increase with the increase of $n$. When the value of $n$ increases from 2 to 16, the hiding capacity increases from 1 bpp to 4bpp, and the embedding rate of FEMD method increases from 1/8 to 1/2, while the embedding rate of our method increases from 1/5 to 8/13. With the same hiding capacity, the embedding rate of the proposed method was 23%-60% higher than that of FEMD respectively. This is because for the same cover image, the auxiliary pixel value is the same, and the encoding number of the stego auxiliary pixel is only determined by its variation, which can be expressed by $(\log_2 n+1)$ bits, and the data amount is obviously less than 8 bits of the cover.

Figure 1. Six test images.
Table 1. Hiding capacity $C$ and embedding rate $E$ of two methods at $n=2^k$.

| $n$ | 2 | 4 | 8 | 16 |
|-----|---|---|---|----|
| $C_1(C_2)$ | 1 bpp | 2 bpp | 3 bpp | 4 bpp |
| $E_1$ | 1/8 | 1/4 | 3/8 | 1/2 |
| $E_2$ | 1/5 | 4/11 | 1/2 | 8/13 |
| $\alpha_E$ | 0.60 | 0.45 | 0.33 | 0.23 |

3.2. PSNR comparison

In order to measure the improvement of image quality in this paper, Table 2 shows the image quality obtained by our method and FEMD method with the same information embedding rate $E$. Overall, our proposed scheme gets higher visual quality than FEMD scheme. Also as it shown that the PSNR of different test images are almost the same, which indicates this kind of hiding scheme is not influenced by the complexity of cover image and has high universality. At different embedding rates, the PSNR is increased by 0.8dB, 1.3dB, 1.1dB and 0.9dB, respectively, with an average improvement of about 1.0dB. In addition, even when 1/2 secret data is embedded, the PSNR of this method is still as high as 35.7dB, which indicates that the algorithm is an efficient data hiding algorithm, and the auxiliary pixel value as the key can ensure the security of the secret data.

Table 2. PSNR(dB) of two methods with the same information embedding rate.

| $n$ | 2 | 4 | 8 | 16 |
|-----|---|---|---|----|
| $E$ | 1/8 | 1/4 | 3/8 | 1/2 |
| Lena | 52.3882 | 46.7534 | 40.8314 | 34.8177 |
| Baboon | 52.3877 | 46.7369 | 40.8207 | 34.8409 |
| Boat | 52.3938 | 46.7411 | 40.8174 | 34.8361 |
| Peppers | 52.4000 | 46.7464 | 40.8370 | 34.8396 |
| Airplane | 52.3940 | 46.7434 | 40.8285 | 34.8442 |
| Goldhill | 52.3969 | 46.7603 | 40.8225 | 34.8326 |
| Average | **52.3934** | **46.7469** | **40.8263** | **34.8352** |

| $E$ | 1/8 | 1/4 | 3/8 | 1/2 |
|-----|---|---|---|----|
| Lena | 53.1903 | 47.9990 | 41.9675 | 35.7089 |
| Baboon | 53.1957 | 48.0085 | 41.9638 | 35.6981 |
| Boat | 53.1894 | 48.0089 | 41.9609 | 35.7193 |
| Peppers | 53.1664 | 48.0013 | 41.9640 | 35.7132 |
| Airplane | 53.1814 | 47.9962 | 41.9817 | 35.7100 |
| Goldhill | 53.1771 | 48.0013 | 41.9761 | 35.7115 |
| Average | **53.1834** | **48.0025** | **41.9690** | **35.7102** |

In addition, in order to compare the algorithm in this paper with other similar algorithms, Lena image hiding effect is compared, and the results are shown in figure 2. As you can see, our scheme and FEMD algorithm can achieve data hiding with different embedding rates, and the visual quality of our algorithm is greater than that of FEMD and other algorithms. Specifically when $n=2$, the PSNR is increased by 2.0dB and 0.8dB respectively compared with LSBs and FEMD algorithm. The reason for the
improvement of image quality is that the data embedding rate in this paper can be greatly improved by adding auxiliary pixels. Compared with the FEMD method, under the condition of embedding the same proportion of secret data, the ratio of pixel pairs used in our method is decreased, so the modification rate of the cover image is reduced.

Figure 2. Comparison results of different data hiding algorithms.

4. Conclusions
We propose a simple and high efficient spatial data hiding algorithm. By adding auxiliary pixel, the bits of the cover pixel pairs can be reduced and the information embedding rate can be improved. When \( n=2^k \), each cover pixel can hide \( k \)-bit secret data, which is equivalent to the LSBs method, but the PSNR of our stego image is increased by 3.5dB on average. By comparing with some similar methods, the performance of this proposed method is improved in both hiding capacity and PSNR.

Acknowledgments
This work is financially supported by the National Natural Science Foundation of China (No.61372175) and the National Key Laboratory Foundation of China (No. HTKJ2019KL504007, No. HTKJ2019KL504006, 2018SSFNKLSMT-13).

References
[1] Mielikainen J 2006 LSB matching revisited IEEE Signal Process. Lett. vol 13 pp 285-7
[2] Zhang X P and Wang S Z 2006 Efficient steganographic embedding by exploiting modification direction IEEE Commun. Lett. vol 10 pp 781-3
[3] Chao R M, Wu H C, Lee C C and Chu Y P 2009 A novel image data hiding scheme with diamond encoding EURASIP J. Inf. Security Vol 2009
[4] Wang J, Sun Y, Xu H, Chen K, Kim H J and Joo S H 2010 An improved section-wise exploiting modification direction method Signal Process. vol 90 pp 2954-64
[5] Kieu T D and Chang C C 2011 A steganographic scheme by fully exploiting modification directions Expert Syst. Appl. vol 38 pp 10648-57
[6] Kuo W C 2013 Image hiding by square fully exploiting modification directions JIHMSP vol 4 pp 128-37
[7] Shen S Y and Huang L H 2015 A data hiding scheme using pixel value differencing and improving exploiting modification directions Comput. Secur. vol 48 pp 131-41
[8] Leng H S 2017 Data hiding scheme based on regular octagon-shaped shells Proc. Int. Conf. on Intelligent Inf. Hiding and Multimedia Signal Process. Springer, Cham vol 81 pp 29-35
[9] Chai X L, Fu X L, Gan Z H, Lu Y and Chen Y R 2019 A color image cryptosystem based on dynamic DNA encryption and chaos Signal Process. vol 155 pp 44-62