IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 24, 2020, accepted November 18, 2020, date of publication November 24, 2020,
date of current version December 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3040048

A Reversible Data Hiding Algorithm Based on Prediction Error With Large Amounts of Data Hiding in Spatial Domain

SHUAI LI[1], LIANG HU[2,3], CHENGYU SUN[2], LING CHI[2,3], TUOHANG LI[2], AND HONGTU LI[2,3]

[1]College of Software Engineering Technology, Jilin University, Changchun 130000, China
[2]College of Computer Science and Technology, Jilin University, Changchun 130000, China
[3]Engineering Research Center of Internet Technology and Software, Ministry of Education, Changchun 130000, China

Corresponding author: Hongtu Li (lihongtu@jlu.edu.cn)

This work was supported in part by the National Key Research and Development Plan of China under Grant 2017YFA0604500, in part by the National Sci-Tech Support Plan of China under Grant 2014BAH02F00, in part by the National Natural Science Foundation of China under Grant 61701190, in part by the Youth Science Foundation of Jilin Province of China under Grant 20160520011JH and Grant 20180520021JH, in part by the Youth Sci-Tech Innovation Leader and Team Project of Jilin Province of China under Grant 20170519017JH, in part by the Key Technology Innovation Cooperation Project of Government and University for the Whole Industry Demonstration under Grant SXGJSF2017-4, in part by the Key Scientific and Technological Research and Development Plan of Jilin Province of China under Grant 20180201103GX, and in part by the Project of Jilin Province Development and Reform Commission under Grant 2019FGWTZC001.

ABSTRACT In recent years among data hiding technologies, Reversible Data Hiding(RDH) technology has attracted widespread interest and application, which is to hide the secret information in a carrier image and recover the original carrier image losslessly to extract the secret information. Current research on RDH algorithms mainly involving frequency domain, spatial domain, and encryption domain. Based on the Prediction-Error Expansion(PEE) methods, as spatial domain approaches, achieved great progress in the past decade. However, there is a defect in the state-of-the-art methods that with the embedded payload increased, the distortion rate of the cover image increased simultaneously. To solve the problem, we proposed a refined reversible data hiding algorithm based on the PEE method with simple implementation. We improved an effective predictor that all the remaining pixels can be predicted in the embedding process, except for those in the first row, the first column, the last row, and the last column in the original image. The extraction process is the reverse of the embedding process that the embedded information and the original carrier is restored without damage. Our work utilized the correlation between image pixels better to solve the inherent contradiction between payload and distortion rate in the state-of-the-art data hiding algorithms. Proven through experiments, our method achieved a large embedding capacity while keeping the image distortion rate and computing complexity low.

INDEX TERMS Reversible data hiding (RDH), prediction-error expansion (PEE), watermarking.

I. INTRODUCTION

With the continuous development of network technology, security issues in telemedicine, intellectual property, information authentication, law,and military use are becoming increasingly important. Regarding network security issues, we first think of modern cryptography. However, cryptography in the traditional sense, its purpose is to make confidential information indecipherable, but it may still be pirated after decryption. After the multimedia content is encrypted, it can be used after decryption. Therefore, to solve this contradiction, information hiding technology has been extensively studied and used. Information hiding is performed to hide secret information in an open carrier. The inspector cannot discern confidential information with the naked eye, and it is more challenging to crack hidden information, as desired for information protection and secret communication. Hence, hidden information is more secure than cryptography. For the

The associate editor coordinating the review of this manuscript and approving it for publication was Amit Singh.

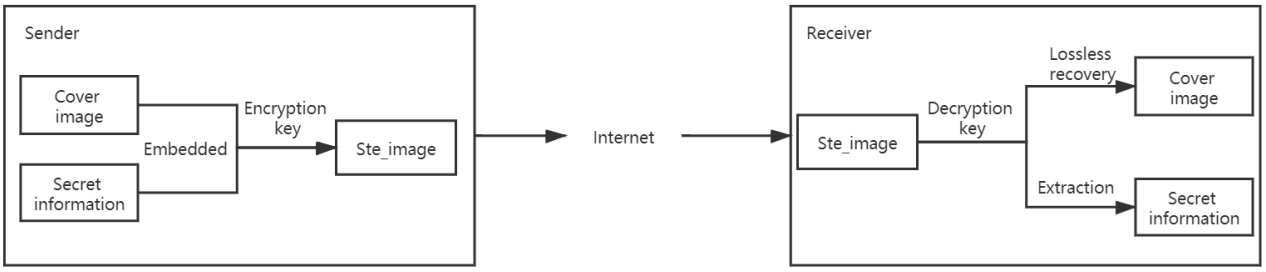


FIGURE 1. Algorithm of the reversible data hiding model.

applications in the fields of medicine, law, the military,and other fields, due to the particularity of these fields, it is required that after a large amount of information is embedded in the carrier, it must still be completely recovered to the original carrier. Therefore, lossless data hiding technology has a more promising future than cryptography. Lossless data hiding is also called reversible data hiding. The typical model of reversible data hiding is shown in Fig. 1.

Reversible data hiding was first proposed by Barton and James [1], and since then, it has been fully developed. Fridrich *et al.* proposed a data hiding algorithm based on lossless compression [2]. However, due to LSB's replacement, the reversible data hiding algorithm with lossless compression obtained a very low compression rate. Therefore, the lossless compression method is inefficient and exhibits poor performance. Subsequently, Tian [3] was the first to propose a difference expansion (DE) embedding algorithm. Compared with the lossless compression algorithm, the DE algorithm did achieve outstanding performance. Although Tian's algorithm was a huge breakthrough at the time, many people worked on it. Based on his research, many improved algorithms were proposed. One of the methods is proposed by Hu *et al.* [4], which is a median edge detector(MED) based on a context-adaptive predictor. However, the DE-based method resulted in relatively low capacity and a certain degree of distortion due to the embedding of position information. The conventional histogram shift algorithm, first proposed by Ni *et al.* [5], selected a pair of peak points and zero points (points with a pixel value of 0) for the statistical characteristics of an image and moved all pixels in this interval to the left or shifted them to the right by one position. As the overall pixel value of the image changed considerably, the image distortion rate became relatively high. Therefore, this method also suffers from limitations. Based on the conventional histogram shifting technique and the DE algorithm, Thodi *et al.* [6] proposed the prediction-error expansion (PEE) method. Compared with the DE-based algorithm, the PEE-based algorithm achieves a better performance.

Wang *et al.* [7] improved the PEE algorithm by shifting the prediction-error histogram left and right, selecting several pairs of peak points and zero points from both sides of the zero point, and selecting a pair of peak points and zero points within a specific range (first, it was shifted to the right, secret information bits were embedded, and then it was shifted to the left for more data embedding). The PEE algorithm can also better solve the distortion caused by the left and right shifts. The remaining pairs are similar. They were combining PEE and histogram shifting results in higher embedding capacity and less distortion. Li *et al.* [8] proposed an adaptive PEE(A-PEE) algorithm, hereafter referred to as the A-PEE algorithm, which can better exploit the redundant space of an image. The difference between the adaptive and conventional algorithms is that Li *et al.* divided the image into two areas, a rough area and a flat area, and selected pixels from these two areas. 1 bit of data can be embedded in the rough area pixels, and 2 bits can be embedded in the flat area pixels. A-PEE method is better used for image features. Sachnev *et al.* [19] used the double-layered embedding. The prediction is made by the average value of four adjacent pixels of a pixel. Gui *et al.* [11] proposed a method based on PEE and an adaptive embedding strategy. The difference is that this method adds a measure of complexity, and the complexity is partitioned into several levels. The size of the embedded data is determined by the complex levels. The experimental results show that Gui's method is better than Li *et al.* [8], Hu *et al.* [4]. Ou *et al.* [9] proposed the P-PEE algorithm based on a 2-dimensional prediction-error histogram(PEH) design. The advantage is that the 2-dimensional PEH can better develop the correlation between the prediction errors, and the method is improved in [10]. The IP-PEE method combines one-dimensional PEH and two-dimensional PEH. A more efficient map is designed to embed secret information. The [25] proposed method has a real-time performance. Besides, several data hiding algorithms based on prediction errors including [12-17,24] and an algorithm based on prediction error hiding for color images [18] are proposed. There are [20-23, 26-31] in the reversible data hiding field worth mentioning recently. After examining many studies by previous researchers, we found that the PEE-based algorithm achieves the best performance among the existing conventional spatial domain reversible data hiding algorithms.

In this article, we proposed an improved prediction error method. We called this method as I-PEE method, which can develop the correlation between image pixels. It is proved through experiments that we have this improvement. The predictor is particularly effective in two aspects: 1. It is an excellent solution to the contradiction in the usual sense of data hiding, achieving a large amount of embedding, low

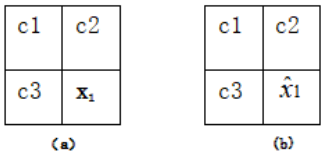


FIGURE 2. Pixel changes in each round of embedding. (a) The original pixels; (b) pixel changes after the first round.

image distortion, and good performance; 2. Low computational complexity with large time overhead. Performance results are reflected in embedding capacity, peak signal to noise rate(PSNR), and Structural Similarity Index Measure (SSIM). Under the 20,000 embedding capacity, our method has an average PSNR higher than 3.52dB. Compared with the prior art, the proposed method can achieve better performance under the same embedding capacity.

The remaining components of the article are presented as follows. The second part describes related works. The suitable application scenario for our proposed method is demonstrated in the third part. The fourth part describes our proposed algorithm and its execution process. The experimental results and discussion are shown in the fifth part to analyze the performance of several spatial domain algorithms combined with PEE. The final part is the conclusion.

II. RELATED WORKS

In this section, the reversible data hiding algorithm based on prediction error is reviewed. The conventional PEE embedding process is divided into the following parts:

1) Predict the original image according to gradient-adjusted prediction(GAP) to obtain the predicted sequence. First, using the scanning command, divide the original image into 2 × 2 nonoverlapping blocks, as shown in Fig.2. Collect a one-dimensional sequence {x1…xn}. Then, obtain the predicted value $\hat{x}i$ according to predictor (1):

$$\hat{x}i = \begin{cases} \max(c2, c3), & if\ c1 \le \min(c2, c3) \\ \min(c2, c3), & if\ c1 \ge \max(c1, c3) \\ c2 + c3 - c1, & otherwise \end{cases} \quad (1)$$

2) Obtain the prediction error through the original pixel value and the predicted value as:

$$ei = xi - \hat{x}i \quad (2)$$

Incorporate the prediction-error value into the prediction-error sequence (ei…en).

3) According to the obtained prediction-error sequence, calculate the frequency of each value to generate a prediction-error histogram, that is, define the histogram as:

$$h(k) = \#\{1 <= i <= N : ei = k\} \quad (3)$$

where # denotes the cardinal number of a set. The distribution of the histogram follows the Laplace distribution, with 0 or a value close to 0 as the center. The sharper the PEH distribution is, the smaller the distortion in the embedded bit.

4) The embedded data are expanded and shifting by modifying PEH. The specific method is as follows:

$$e'i = \begin{cases} 2ei + b, & if\ ei \in [-T, T) \\ ei + T, & if\ ei \in [T, +\infty) \\ ei - T, & if\ ei \in (-\infty, -T] \end{cases} \quad (4)$$

where T is a parameter that is determined according to the embedding capacity.$b \in \{0, 1\}$is the secret information bit used for embedding, and e'i is the denoted prediction error obtained after embedding and shifting.

5)Finally, obtain the pixel value of the encrypted image donated Spixel according to the prediction error and the pixel prediction value.

$$Spixel = \hat{x}i + e'i \quad (5)$$

III. APPLICATION SCENARIO

The purpose of the method proposed in this paper is to prevent the information from being intercepted completely during the Internet transmission process. And when the receiving end receives the image, the information can be extracted losslessly, and the original image can be restored.

Scenario 1: In the transmission of secret military information, the sender can embed large-capacity secret information data into an image in multiple layers through this method. During the Internet transmission, if the image is intercepted by the attacker and the secret key is also not known. It is difficult to decipher and extract the original information.

Scenario 2: In order to facilitate the diagnosis by doctors, in the telemedicine network, patient medical image information and medical records need to be transmitted to medical experts via the Internet, and then the experts transmit the diagnosis information to the patient. However, in the process of network transmission, the patient's private information is easy to leak. In order to prevent the occurrence of the above situation, the information can be embedded in the medical image. The patient (doctor) can embed the medical record information (diagnostic information) into the image through the multi-layer embedding method proposed in this article, which can prevent the information from being completely intercepted. Due to the sensitivity of medical images, small changes in the images may cause serious medical accidents. This method can ensure that the original image can be restored losslessly after the information is extracted.

The above two application scenarios are mainly composed of two stages:

The first stage: the sender sends the encrypted image generated by the encryption key to the sender in a secure way as far as possible to prevent interception by attackers.

The second stage: the receiver can losslessly extract the information transmitted by the sending end and restore the original image after receiving the image.

IV. PROPOSED METHOD

The I-PEE algorithm partitions the carrier image and divides it into two areas: the shadow area and the blank area. First,

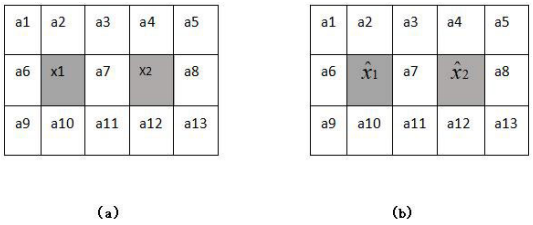


FIGURE 3. Pixel changes in each round of embedding.(a) Original pixel value (b) Predicted shadow area pixels value.

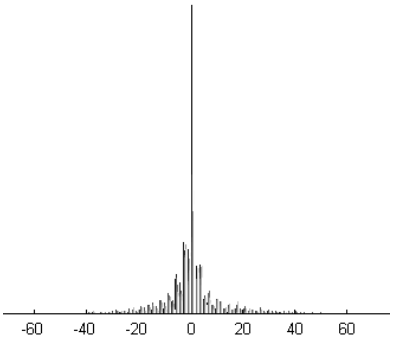


FIGURE 4. Lena's prediction error histogram.

the first layer of embedding is performed on the pixels in the shadow area. Then, the blank pixels can be embedded in multiple layers. The blank area can be embedded up to 3 layers.

A. EMBEDDING PROCEDURE

This section describes the first layer of the shadow area embedding procedure as follows:

1) Scan the carrier image sequentially by using scanning commands from left to right and top to bottom to obtain the original pixel sequence {x1…,xn}.

Predict the pixel value through (6). Here, our image is predicted in the form of the Fig.3. We obtain a one-dimensional prediction sequence{$\hat{x}1, \hat{x}2, \hat{x}3, \ldots\ldots, \hat{x}n$}

$$\hat{x}n(i,j) = \left\lfloor \begin{pmatrix} a(i-1,j-1)+a(i-1,j) \\ +a(i-1,j+1)+a(i,j-1) \\ +a(i,j+1)+a(i+1,j-1) \\ +a(i+1,j)+a(i+1,j+1) \end{pmatrix} \Big/ 8 \right\rfloor \quad (6)$$

where i and j respectively represent the row and column of the current pixel. {a1, a2…, an} are all original pixel values in the first layer of embedding, and the predicted values obtained here are all regarded as integers.

2) Generate a prediction-error histogram based on the prediction-error values. The prediction-error sequence {e1…,en} is obtained according to formula (2) with the obtained prediction value. Then, obtain the prediction-error histogram according to the prediction-error sequence. The first row, the first column, the last row and the last column of the pixels of the carrier image are not calculated for prediction, so their prediction-error value is regarded as zero. As shown in Fig.4.

3) Embed additional information to obtain the encrypted prediction-error histogram. The additional information includes the length parameter of the secret information and the size of the compressed location map.

Location map: To prevent the greyscale image from overflowing and underflowing after embedding information, that is, to prevent it from exceeding the range of [0, 255], we adjust the pixel value within a reliable range. Therefore, in our method, the modification of each pixel value is at most 1, only need to adjust the boundary pixels value. For example, modify the value of xi from 255 to 254 and the value of xi from 0 to 1. Change the location map corresponding to the modified pixel to 1 and the location map corresponding to the remaining unmodified pixels to 0. Then, the obtained location map is losslessly compressed.

In our method, the additional information is finally embedded in the first line through LSB replacement, and the information of the first line is the first to be extracted. Therefore, the replaced LSB of the first line, the compressed location map, and the secret information are embedded in the cover image as part of the effective payload.

The secret information $b \in \{0, 1\}$ is embedded in the prediction error, and the expanded and shifted prediction-error values are the same as in (4). Here, we choose 1 to be the value of T. We set the embeddable range to $[-1, 1)$, and the expandable range to $(-\infty, -1)$ and $[1, +\infty)$by 1 bit to the left and right within the range until the end of the additional information embedding.

4) Finally, each shadow pixel can get an encrypted pixel value after embedding and translation. According to formula (7), an encrypted image can be obtained.

$$x'i = \hat{x}i + e'i \quad (7)$$

Similarly, the I-PEE method can be embedded in multiple layers, as shown in Fig3(a), where the blank part can be embedded in up to three layers.

Multi-layer embedding process of the blank part:

1) Calculate the pixel prediction value. The difference with the shaded part is that the pixel value prediction of the blank part is based on the pixel value of the previous layer of the encrypted image. When embedding in the second layer, select the blank pixels x(i,j+1), x(i+1,j), x(i+1,j+1) adjacent to the shadow pixel x(i,j) for embedding, Use the same prediction method Formula 6 for prediction. The value used to participate in the prediction of the second layer during embedding is the modified value during the embedding of the first layer.

2) Calculate the prediction error value. That is, the difference between the original pixel value of the current blank part of the pixel and its predicted value obtains the prediction error value sequence. According to the obtained prediction error sequence, the frequency of each value is calculated to generate the prediction error histogram of the second layer of pixels (Fig.4). The embedded data is expanded and translated by modifying the prediction error histogram.

3) Perform data embedding and translation according to the prediction error map. The anti-overflow treatment has

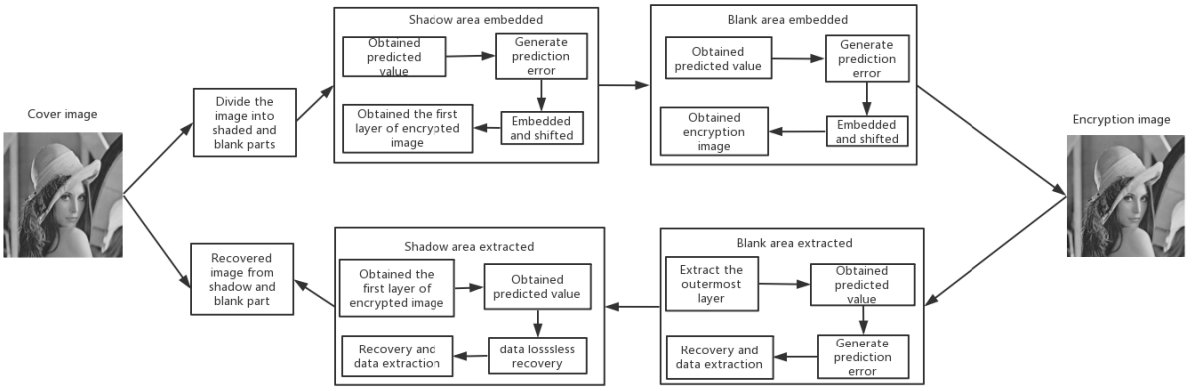


FIGURE 5. Flow chart of the embedding and extraction processes of our proposed algorithm.

already been done in the first layer of embedding, so there is no need to do it again. That is, there is no need to compress the position map.

4) The blank pixels are embedded and translated to obtain an encrypted image.

We should noted that if two-layer embedding is used, it is best to divide the secret information into two parts of a similar size and then perform corresponding data embedding and shifting on the entire information. The flow chart of our method embedding and extraction as shown in Fig.5.

B. EXTRACTION PROCEDURE

This section is the corresponding extraction process. In the process of extracting, first, extract the secret information embedded in the outermost layer, and then sequentially extract to the inner layer. After the extraction process, the original image can finally be recovered losslessly and get the secret information completely.

The process of extracting the outermost information in the blank part:

1) Extract the additional information and length parameter of the secret information from the first line by reading the LSB of the first line of the encrypted image to obtain the actual effective load capacity in the image. Recover the replaced LSB to restore the original values in the first row of pixels.

2) Use the same prediction or scanning order to obtain the prediction pixel values of the encrypted image in which denoted p's, then obtained the prediction-error value of the encrypted image marked d's, which is the same process as in the embedding stage.

$$d's = x'i - p's \tag{8}$$

3) Extract the secret information first. According to the obtained prediction-error value d's(i,j) and extract the secret information at the range of $[-2, 1)$ base on T=1, as following:

$$S = mod(d's(i,j) + 1, 2) \tag{9}$$

$$pr(i,j) = (p's(i,j)) + (d's(i,j) - S)/2 \tag{10}$$

where S is the extracted secret information bit, pr is the recovered pixel value.End until all the secret information is extracted.In the range of expandable pixels,due to without the embedding information,only shifting 1 bit left or right as following:

$$\begin{cases} pr(i,j) = p's(i,j) + d's(i,j) - T \\ \qquad\qquad if\ \ d's(i,j) \in [1, +\infty) \\ pr(i,j) = p's(i,j) + d's(i,j) + T \\ \qquad\qquad if\ \ d's(i,j) \in (-\infty, -2) \end{cases} \tag{11}$$

Until the extraction of all secret information in the blank part is completed.

4) Recover the pixel value of the outermost encrypted image.

The process of extracting the information in the shadow area:

1) After extracting the information of the blank part in the previous, the encrypted image of the first layer of the shadow part is obtained, and the same prediction or scanning command is used to obtain the pixel prediction value p's of the encrypted image, and then the mark prediction error of the encrypted image is obtained The value d's is the same as the blank extraction.

2) Extract secret information according to the obtained prediction error sequence. The process is the same as the blank area extraction.

3) Extract all the information, and finally decompresses the lossless compressed position map to obtain the decompressed position map. According to the decompressed position map, the pixel with the corresponding position marked as 1 is obtained, which is modified and restored to recover the original pixel value.

4) Recover the original image losslessly and get the secret information.

According to the above process, the original image and encrypted information can be recovered losslessly. Here, the first rows, first columns, last row, and last columns of the original image and the encrypted image have not changed during the embedding and extraction processes.

(a) (b) (c) (d) (e) (f)

FIGURE 6. The test images are downloaded from USC-SIPI (512 × 512): (a)Lena, (b)Baboon, (c)Barbara, (d)Airplane, (e)Lake and (f)Boat.

The predicted value of the encrypted image is the same as the predicted value of the original image.

V. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we conduct experiments on different gray-scale images of the same size. The images used in the test are shown in Fig.6. Except for Barbara, the test images are all 8-bit 512 × 512 gray-scale images from the USC-SIPI image database. In addition, we also tested in the BOSSbase and in the MedPix database. BOSSbase has been widely utilized in information hiding, and the MedPix database contains a lot of medical images. The experimental environment is MATLAB R2014b, and the processor platform is an Intel Core i7-8700 (3.19 GHz).

In the performance analysis, we adopt PSNR and SSIM as the measurement standards. The calculation method of PSNR is:

$$PSNR = 10\log 10(\frac{255^2}{MSE}) \tag{12}$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[P(i,j) - P's(i,j)\right]^2 \tag{13}$$

where MSE is the mean square error between the original image P and the encrypted image P'. M and N are the width and height of the original image, respectively.

Wang [31] introduced a metric named SSIM. SSIM is used as an index to evaluate image structure information, ranging from -1 to 1. When the SSIM value is 1, it means that the compared images are the most similar. The calculation formula of SSIM between two images is:

$$SSIM(P, P'S) = \frac{(2\mu p\mu p's + c1)(2\sigma pp's + c2)}{(\mu_p^2 + \mu_{p's}^2 + c1)(\sigma_p^2 + \sigma_{p's}^2 + c2)} \tag{14}$$

where μP and $\mu P's$ are the mean of images P and P's respectively. Where σ_P^2 and $\sigma_{P's}^2$ are the variance of images P and P's, respectively. $\sigma pp's$ is the covariance of images P and P's. c1 and c2 are predefined constants:

$$\begin{cases} c1 = (k1L)^2 & where \;\; k1 << 1 \\ c2 = (k2L)^2 & where \;\; k2 << 1 \end{cases} \tag{15}$$

where L is the range of pixels.

Here, we compare the performance of our proposed algorithm I-PEE with the experiments with the A-PEE, P-PEE, and IP-PEE algorithms (Li *et al.*[8] (2011), Ou *et al.*[9] (2013), [10] (2019)). Fig. 7 shows the performance comparison results of different algorithms on the same image, where the abscissa is EC, and the ordinate is PSNR. The different methods are to embed data starting from 5,000, and each embedding step is 5,000.

According to Table.1, when the capacity is 15,000, our method lower than P-PEE is 0.33dB, and lower than IP-PEE(FM), IP-PEE(AMG), IP-PEE(AMO) are 0.33dB, 0.79dB and 1.43dB, respectively. However, higher than the A-PEE method is 0.8dB. On the contrary, when the capacity is 5,5000, our method is higher than P-PEE, A-PEE, IP-PEE(FM), IP -PEE(AMG), IP-PEE(AMO) are 1.25dB, 2.7dB, 1.07dB, 0.82dB, and 0.80dB, respectively. According to Table 2, when the capacity is 15,000, our method is higher than P-PEE, A -PEE, IP-PEE(FM), IP-PEE(AMG), IP-PEE(AMO) are 3.49dB, 4.52dB, 3.17dB, 2.68dB and 2.53dB, respectively. When the capacity is 5,5000, Our method is higher than P-PEE, A-PEE, IP-PEE(FM), IP-PEE(AMG), IP-PEE(AMO) are 4.53dB, 5.55dB, 4.13dB, 3.83dB and 3.94dB, respectively. Compared with other methods, the I-PEE algorithm is 3.81dB higher on average. It can be seen from Fig.7 that when the embedding rate is low, and the embedding payload capacity is 5,000, our algorithm has a lower PSNR. When the embedding capacity is lower than 50,000, our algorithm performance is not good for some pictures. The reason is our algorithm cannot make good use of the correlation between pixels when the embedding capacity is low. As the embedding capacity increases, our method has the highest PSNR and the lowest distortion rate than other methods when the embedding amount is greater than 50,000. According to the performance comparison with other algorithms shown in Fig.7, it is clear that our method has a higher PSNR than other algorithms as the number of embedded data increases, and the image distortion rate is low. Therefore, our algorithm has better performance when large amounts of data are hidden.

According to Table.2, when Li's A-PEE method's embedded capacity is 5,000, the PSNR is 64.13dB, which is 1.81dB lower than our algorithm. Compared with P-PEE, IP-PEE(FM), IP-PEE(AMG), the IP-PEE (AMO) algorithm is higher than 1.03dB, 0.74dB, 0.23dB and 1.82dB respectively. When the capacity is 5,5000, compared with I-PEE, P-PEE, IP-PEE(FM), IP-PEE(AMG), IP-PEE(AMO) algorithm, it is lower 5.55dB, 1.02dB,1.42dB, 1.72 dB and 1.61dB, respectively. A-PEE method can not achieve a good performance,

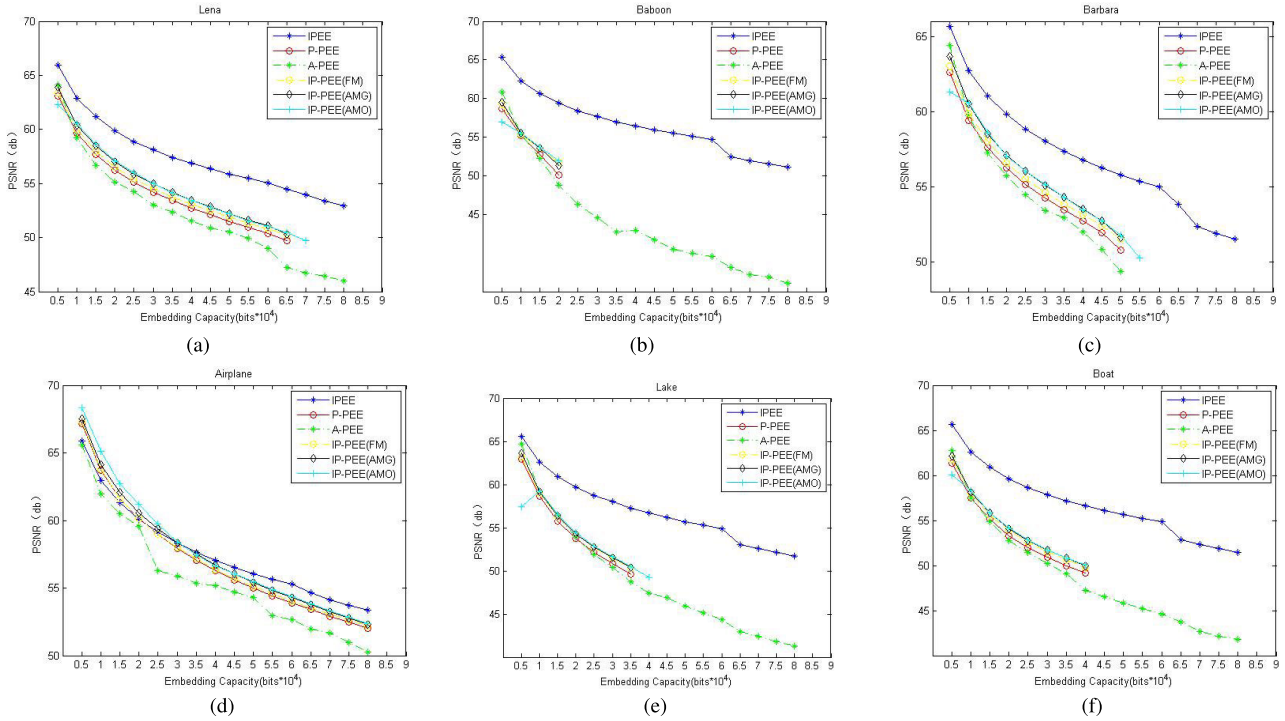


FIGURE 7. Comparison of embedding capacity and image quality:(a) Lena, (b)Baboon, (c)Barbara, (d)Airplane, (e)Lake, and (f)Boat.

TABLE 1. Comparison of PSNR values (dB) between our proposed method and other five methods when using Airplane for $EC \times 10^4$.

Method \ EC	0.5	1.5	2.5	3.5	4.5	5.5	6	6.5
I-PEE	65.90	61.30	59.15	57.64	56.52	55.65	55.27	54.62
P-PEE	67.17	61.63	58.94	57.05	55.61	54.40	53.91	53.40
A-PEE	65.59	60.50	56.30	55.36	54.72	52.95	52.64	51.95
IP-PEE(FM)	67.27	61.63	58.99	57.14	55.70	54.58	54.02	53.55
IP-PEE(AMG)	67.54	62.09	59.40	57.54	56.03	54.83	54.29	53.76
IP-PEE(AMO)	68.34	62.73	59.74	57.47	56.04	54.85	54.35	53.81

TABLE 2. Comparison of PSNR values (dB) between our proposed method and other five methods when using Lena for $EC \times 10^4$.

Method \ EC	0.5	1.5	2.5	3.5	4	4.5	5.5	6.5
I-PEE	65.94	61.16	58.88	57.42	56.85	56.33	55.46	54.47
P-PEE	63.10	57.67	55.13	53.41	52.73	52.09	50.93	49.68
A-PEE	64.13	56.64	54.21	52.35	51.55	50.89	49.91	47.25
IP-PEE(FM)	63.39	57.99	55.43	53.76	53.05	52.46	51.33	50.21
IP-PEE(AMG)	63.90	58.48	55.88	54.16	53.46	52.83	51.63	50.31
IP-PEE(AMO)	62.31	58.63	56.01	54.08	53.44	52.78	51.52	50.43

because this method is an image adaptive steganography algorithm, embed more bits are mainly concentrated in the smooth area, it to be selected the area in which is not easy for detected by the attacker for embedding secret information according to the characteristics of the carrier image content. Therefore, the embedded payload size has different limitations on different image content, and the threshold selection of the algorithm has a great relationship with the image itself. Therefore, when Li's method is compared with other algorithms, as the embedding capacity increases, the PSNR

TABLE 3. The PSNR of our proposed method is compared with the other 5 methods when the EC is 20,000.

Image \ Method	A-PEE	P-PEE	IP-PEE(FM)	IP-PEE(AMO)	IP-PEE(AMG)	Proposed
Lena	55.16	56.23	56.55	57.09	57.01	59.88
Baboon	48.72	50.11	51.69	51.93	51.28	59.37
Barbara	55.72	56.22	56.57	57.04	57.06	59.8
Airplane	59.53	60.17	60.17	61.22	60.55	60.09
Lake	53.86	53.70	54.22	54.39	54.29	59.71
Boat	52.79	53.33	53.87	54.16	54.08	59.61
Average	**54.30**	**54.96**	**55.51**	**55.97**	**55.71**	**59.74**

TABLE 4. SSIM comparison between different algorithms using 6 test grayscale images at a capacity of 5,000.

Image \ Method	I-PEE	A-PEE	P-PEE	IP-PEE(FM)	IP-PEE(AMG)	IP-PEE(AMO)
Boat	0.9999	0.9998	0.9999	0.9971	0.9975	0.9999
Lena	0.9999	0.9998	0.9999	0.9966	0.9971	0.9999
Barbara	0.9999	0.9999	0.9999	0.9970	0.9975	0.9999
Lake	0.9999	0.9998	0.9999	0.9961	0.9965	0.9998
Airplane	0.9999	0.9998	0.9999	0.9927	0.9929	0.9999
Baboon	0.9999	0.9998	0.9998	0.9987	0.9988	0.9999

TABLE 5. SSIM comparison between different algorithms using 6 test grayscale images at a capacity of 20,000.

Image \ Method	I-PEE	A-PEE	P-PEE	IP-PEE(FM)	IP-PEE(AMG)	IP-PEE(AMO)
Boat	0.9998	0.9995	0.9996	0.9918	0.9925	0.9997
Lena	0.9998	0.9995	0.9997	0.9892	0.9905	0.9997
Barbara	0.9999	0.9997	0.9997	0.9903	0.9915	0.9998
Lake	0.9999	0.9995	0.9997	0.9884	0.9893	0.9997
Airplane	0.9998	0.9995	0.9998	0.9810	0.9825	0.9998
Baboon	0.9999	0.9990	0.9996	0.9968	0.9969	0.9997

is also the lowest. The P-PEE algorithm and the IP-PEE algorithm proposed by Ou *et al.* extend one-dimensional PEH to two-dimensional PEH in the embedding process. The advantage of the extended prediction-error pair is that the direction of information embedding and expansion can be adjusted adaptively to reduce distortion. The direction of information embedding follows the direction with the smallest change in error,reducing distortion. However, in the adaptive embedding process, the choice of the threshold also affects the algorithm's performance. In contrast, we propose that the algorithm does not affect the payload's size because of the image itself. IN the I-PEE algorithm, the maximum payload capacity of a 512×512 grayscale image is 509×509. In the first layer of embedding, we can obtain a maximum effective capacity of 65,025. After the second layer of embedding, we can obtain a maximum capacity of 130,050, and so on. From Table.3, our method is mostly higher than other algorithms under the same embedding capacity PSNR for different images. Under the embedding capacity of 20,000, our method has an average PSNR higher than 3.52dB.

According to Table.4 and Table.5, we performed SSIM analysis to illustrate the structural differences between the original image and the embedded image in various algorithms under the same capacity. When the capacity is 5,000, the structure of our algorithm under different images is maintained at 0.9999, which means the image structure of our algorithm is well protected after embedding information. In contrast, other algorithms have relatively satisfying performance at low capacity. As the capacity increases, our algorithm SSIM is still relatively stable at 0.9999 when the capacity is 20,000. In contrast, the SSIM of other algorithms under different images is lower than our algorithm.

Finally, the proposed method does not take much time to execute by Matlab and a personal computer for computational complexity. A-PEE, P-PEE, IP-PEE (FM), IP-PEE (AMG), and IP-PEE (AMO) of the embedding process takes an average of 23 seconds, 11 seconds, 11 seconds, 18 seconds, and 64 seconds, respectively, but our method takes only 10 seconds on average. The time overhead is also relatively low.

VI. CONCLUSION

In recent years, with the increasing demand for data security, reversible data hiding technology plays an active role in promoting the development and application of information security technology. RDH technology based on the PEE algorithm has attracted the attention of researchers and achieved many results. The reversibility of reversible information hiding focuses on the lossless decryption of text carried by the password and the recovery of the carrier without distortion.

This paper briefly introduced the key technology of the conventional PEE algorithm. All the above methods in this paper are reversible, and the inverse process is the reverse operation of the embedding process. Through the experimental and discussion of related typical algorithms, compares the performance measurements of several methods from the perspective of embedding ability and visual image quality. Our proposed reversible data hiding algorithm ''I-PEE'' based on the spatial domain possesses a little time overhead. And during the embedding process, the first row pixels, the first column pixels, the last row pixels, and the last column pixels of the original image remain unchanged. The prediction results are the same during the embedding and extraction processes. Thus, except for the first column pixels, the first row pixels, the last column pixels, and the last row pixels, the remaining pixels can be predicted, so large-capacity information embedding can be carried out, and a relatively good PSNR can be obtained when getting a large embedding payload. The secret information can be extracted correctly, and the original image can be recovered losslessly.

Our main contribution is in this article, which is reflected in the ability to develop the correlation between image pixels and propose an efficient PEE predictor. Solved the contradiction inherent in the usual sense of data hiding: It achieves a large amount of embedding while keeping the image distortion rate low. It exhibits good performance and has low computational complexity requires no large time overhead. Compared with the prior art, the proposed method can achieve better performance under the same embedding capacity. Our further work aimed at the refinement on the security of reversible data hiding algorithms. Moreover, we focused on applying Generative Adversarial Networks(GAN), an state-of-the-art deep learning model, to improve our algorithms for better perfromance.

REFERENCES

[1] J. M. Barton, ''Method and apparatus for embedding authentication information within digital data,'' Sony Corp., New York, NY, USA, Tech. Rep. 6115818, 2003.

[2] M. Goljan, J. Jessica Fridrich, and R. Du, ''Distortion-free data embedding for images,'' in *Proc. Int. Workshop Inf. Hiding*, 2001, pp. 27–41.

[3] J. Tian, ''Reversible data embedding using a difference expansion,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[4] Y. Hu, H.-K. Lee, and J. Li, ''DE-based reversible data hiding with improved overflow location map,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 2, pp. 250–260, Feb. 2009.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, ''Reversible data hiding,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[6] D. M. Thodi and J. J. Rodriguez, ''Expansion embedding techniques for reversible watermarking,'' *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[7] W. Wang, J. Ye, T. Wang, and W. Wang, ''A high capacity reversible data hiding scheme based on right-left shift,'' *Signal Process.*, vol. 150, pp. 102–115, Sep. 2018.

[8] X. Li, B. Yang, and T. Zeng, ''Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,'' *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[9] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, ''Pairwise prediction-error expansion for efficient reversible data hiding,'' *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[10] B. Ou, X. Li, W. Zhang, and Y. Zhao, ''Improving pairwise PEE via hybrid-dimensional histogram generation and adaptive mapping selection,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 7, pp. 2176–2190, Jul. 2019.

[11] X. Gui, X. Li, and B. Yang, ''A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding,'' *Signal Process.*, vol. 98, pp. 370–380, May 2014.

[12] J. Xu, H. Zhou, W. Zhang, R. Jiang, G. Ma, and N. Yu, ''Second order perdicting-error sorting for reversible data hiding,'' in *Digital Forensics and Watermarking*, vol. 10082. Beijing, China, 2017, pp. 407–420, doi: 10.1007/978-3-319-53465-7.

[13] S. Yi, Y. Zhou, and Z. Hua, ''Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion,'' *Signal Process., Image Commun.*, vol. 64, pp. 78–88, May 2018.

[14] J. Hsiao, C. Yuan, Z. Y. Lin, and P. Y. Chen, ''Reversible data hiding based on pairwise prediction-error histogram,'' *J. Inf. Sci. Eng.*, vol. 33, no. 2, pp. 289–304, Mar. 2017.

[15] P. Puteaux and W. Puech, ''An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images,'' *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

[16] X.-Z. Xie, C.-C. Chang, and Y.-C. Hu, ''An adaptive reversible data hiding scheme based on prediction error histogram shifting by exploiting signed-digit representation,'' *Multimedia Tools Appl.*, vol. 79, nos. 33–34, pp. 24329–24346, Sep. 2020.

[17] A. Malik, H.-X. Wang, Y. Chen, and A. N. Khan, ''A reversible data hiding in encrypted image based on prediction-error estimation and location map,'' *Multimedia Tools Appl.*, vol. 79, nos. 17–18, pp. 11591–11614, May 2020.

[18] Y. Qi and L. Liu, ''Reversible watermarking algorithm based on prediction error expansion for color image,'' in *Proc. 32nd Youth Academic Annu. Conf. Chin. Assoc. Automat. (YAC)*, May 2017, pp. 102–105.

[19] V. Sachnev, H. Joong Kim, J. Nam, S. Suresh, and Y. Qing Shi, ''Reversible watermarking algorithm using sorting and prediction,'' *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

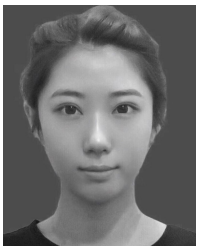
[20] F. Di, F. Huang, M. Zhang, J. Liu, and X. Yang, ''Reversible data hiding in encrypted images with high capacity by bitplane operations and adaptive embedding,'' *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 20917–20935, Aug. 2018.

[21] Z. Yin, Y. Peng, and Y. Xiang, ''Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression,'' *IEEE Trans. Dependable Secure Comput.*, early access, Aug. 26, 2020, doi: 10.1109/TDSC.2020.3019490.

[22] Q. Li, B. Yan, H. Li, and N. Chen, ''Separable reversible data hiding in encrypted images with improved security and capacity,'' *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30749–30768, Dec. 2018.

[23] A. Malik, H. Wang, H. Wu, and S. M. Abdullahi, ''Reversible data hiding with multiple data for multiple users in an encrypted image,'' *Int. J. Digit. Crime Forensics*, vol. 11, no. 1, pp. 46–61, Jan. 2019.

[24] Z. Tang, S. Xu, H. Yao, C. Qin, and X. Zhang, "Reversible data hiding with differential compression in encrypted image," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 9691–9715, Apr. 2019.
[25] Z. Tang, S. Xu, D. Ye, J. Wang, X. Zhang, and C. Yu, "Real-time reversible data hiding with shifting block histogram of pixel differences in encrypted image," *J. Real-Time Image Process.*, vol. 16, no. 3, pp. 709–724, Jun. 2019.
[26] J. Wang, "Rate and distortion optimization for reversible data hiding using multiple histogram shifting," *IEEE Trans. Cybern.* vol. 47, no. 2, pp. 315–326, Feb. 2017.
[27] H. Yao, X. Liu, Z. Tang, Y.-C. Hu, and C. Qin, "An improved image camouflage technique using color difference channel transformation and optimal prediction-error expansion," *IEEE Access*, vol. 6, pp. 40569–40584, 2018.
[28] Z. Yin, A. Abel, J. Tang, X. Zhang, and B. Luo, "Reversible data hiding in encrypted images based on multi-level encryption and block histogram modification," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3899–3920, Feb. 2017.
[29] W. Zhang, P. Kong, H. Yao, Y.-C. Hu, and F. Cao, "Real-time reversible data hiding in encrypted images based on hybrid embedding mechanism," *J. Real-Time Image Process.*, vol. 16, no. 3, pp. 697–708, Jun. 2019.
[30] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.
[31] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.



SHUAI LI was born in 1996. She received the B.S. degree in computer science and technology from the Changchun Institute of Technology. She is currently pursuing the master's degree with the College of Software Engineering, Jilin University (JLU). Her research interests include network security, machine learning, NLP, and data mining.

LIANG HU was born in 1968. He received the B.S. degree from the Harbin Institute of Technology (HIT), Harbin, and the M.S. and Ph.D. degrees from the College of Computer Science and Technology, Jilin University (JLU), Changchun, China. He has been a Professor with JLU, since 2002, where he has been a Ph.D. Supervisor since 2003. His current research interests include distributed computing, network computing and security, and data security and privacy.

CHENGYU SUN was born in 1995. He received the B.S. degree from the College of Software Engineering, Dalian Jiaotong University (DJTU). He is currently pursuing the master's degree with the College of Computer Science and Technology, Jilin University. His current research interests include NLP, data mining, and machine learning.

LING CHI received the B.S. degree from the Mathematics School and Institute, Jilin University, and the M.S. and Ph.D. degrees from the College of Computer Science and Technology, Jilin University. He was a Lecturer with Jilin University. His research interests include network security, cryptography, wireless network security, machine learning, data mining, data processing, and NLP.

TUOHANG LI was born in 1994. He received the B.S. degree from the College of Electronic Science and Engineering, Jilin University (JLU), and the M.S. degree from the Department of Electrical and Electronic Engineering, University of Bristol (UoB). He is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Jilin University. His current research interests include machine learning, NLP, and knowledge graph.

HONGTU LI was born in 1984. He received the Ph.D. degree from the College of Computer Science and Technology, Jilin University (JLU), Changchun, China. He has been a Lecturer with Jilin University since 2012. His current research interests include cryptography, data integrity protection, wireless network security, and data processing.