Signal Processing 89 (2009) 1129–1143

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Reversible image hiding scheme using predictive coding and histogram shifting

Piyu Tsai [a], Yu-Chen Hu [b,*], Hsiu-Lien Yeh [a]

[a] *Department of Computer Science and Information Engineering, National United University, Miaoli, Taiwan 360, ROC*
[b] *Department of Computer Science and Information Management, Providence University, Taichung, Taiwan 433, ROC*

ARTICLE INFO

Article history:
Received 7 April 2008
Received in revised form
17 December 2008
Accepted 19 December 2008
Available online 30 December 2008

Keywords:
Reversible data hiding
Predictive coding
Image histogram
Histogram shifting

ABSTRACT

In this paper, a reversible image hiding scheme based on histogram shifting for medical images is proposed. As we know, the histogram-based reversible data hiding is limited by the hiding capacity, which is influenced by the overhead of position information that has to be embedded in the host image. To solve this problem, the similarity of neighboring pixels in the images was explored by using the prediction technique and the residual histogram of the predicted errors of the host image was used to hide the secret data in the proposed scheme. In addition, the overlapping between peak and zero pairs was used to further increase the hiding capacity.

According to the experimental results, a higher hiding capacity was obtained and a good quality stego-image was preserved in the proposed scheme. The hiding capacity provided by the proposed scheme was approximately three times that of the original histogram-based method. Compared to the histogram-based method, the quality of the stego-image improved about 1.5 dB when the same amounts of secret data were embedded.

Crown Copyright © 2009 Published by Elsevier B.V. All rights reserved.

1. Introduction

The popularity of networking has made the distribution of the digital media easier and faster. Security problems, such as modification, forgery, duplication, interception and others, on the Internet have reached critical proportions [1,2]. Several approaches have been proposed to protect the security of digital media. Data hiding conceals the secret message on the cover medium for property right protection, authentication, secret sharing and so on. The secret message can be extracted to prove the ownership or to verify the content integrity or to secretly transmit the message [1].

Quite a few data hiding schemes modify the original medium to embed the secret message without the capability to recover the host medium after the secret message is extracted [1–11]. However, reversible recovery of the cover medium is essential or preferable for some multimedia applications such as medical diagnosis, law enforcement, fine art work and so on. For example, in an image for law enforcement, the authentication message must be embedded. Lossless recovery of the original image is required after the authentication message is extracted. In fine art work, the watermark is usually embedded in the digital medium for ownership protection. It is preferable that the original medium be recovered after the watermark is extracted.

Nowadays, research in reversible data hiding has become quite important. Several reversible data hiding schemes have been proposed [12–21]. These schemes can be divided according to three approaches: spatial domain, frequency domain, and index-based domain. In the spatial

[*] Corresponding author. Tel.: +886 4 26328001x18112; fax: +886 4 26324045.
E-mail addresses: pytsai@nuu.edu.tw (P. Tsai), ychu@pu.edu.tw (Y.-C. Hu), showlien@nuu.edu.tw (H.-L. Yeh).

0165-1684/$ - see front matter Crown Copyright © 2009 Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2008.12.017

domain approach, Celik et al. employed a generalized least significant bit (LSB) method and the context-based adaptive lossless image coding (CALIC) to achieve reversible data hiding [12]. In their method, the original pixel value was transformed by using prediction processing. The residual values and the secret data were compressed using CALIC and were then embedded via the generalized LSB modification method.

A difference expansion data hiding is proposed by Tian in 2003 [13]. In this scheme, the redundancy of the pixels was explored to achieve a high hiding capacity. The difference and average values of two neighboring pixels were calculated. The secret data to be embedded was appended to a difference value represented as a binary number. In other words, the difference value was first multiplied with 2. Then the addition of the difference value and 1-bit secret data was calculated. The result was stored in the difference value. Two neighboring pixels were replaced with the summation and subtraction of the average value and half of the expanded difference value, respectively.

In addition, the histogram of the pixels in the cover image was explored by Ni et al. [14] to design a reversible hiding scheme in 2006. The peak and zero pair of the histogram were searched. The pixels between the peak and zero pair were modified in the embedding processing. The pixel in the peak point was used to carry a bit of the secret message. The others were modified and no secret data were embedded. In the histogram-based data hiding, the number of pixels in the peak point is the maximal hiding capacity for the secret message to be embedded. More of the peak and zero pairs were selected to enhance the hiding capacity. Also, a reversible binary image data hiding was proposed by Tsai et al. [15] in 2005. The pairwise logical computation (PWLC) mechanism for data hiding was introduced. This scheme achieved high hiding capacity and low visual quality degradation.

In the frequency domain approach, some reversible data hiding schemes that embedded the secret data in the transformed coefficients was introduced. Fridrich et al. [16] proposed LSB-based reversible data hiding in 2001. The LSB bit plane of the quantized DCT coefficients was compressed with an adaptive context-free lossless arithmetic compression algorithm. The compressed data along with the secret message were then embedded in the LSB bits of the selected coefficients. In this method, the lossless codec was used to save storage space so that the secret data could be embedded.

In 2002, Xuan et al. [17] explored the relationship between the bit-planes of the integer discrete wavelet transformation (IDWT) coefficients to design a reversible data hiding scheme. The middle and high frequency subbands of IDWT coefficients in the middle bit planes were compressed by using arithmetic coding algorithm. Secret data and the compressed coefficients were then embedded in these selected sub-bands. In 2005, Kamstra and Heijmans's [18] proposed a data hiding scheme that employed DWT coefficients to carry the secret data. The DWT coefficients in lower sub-bands were sorted according to the variance values. Then, Tian's scheme [13] was applied to process the sorted DWT coefficients, such that the original DWT coefficients could be reconstructed completely.

In the index domain approach, secret data was embedded in the vector quantized digital medium. After extracting the secret data, the vector quantized codes also had to be reconstructed. In 2005, a data hiding scheme based on vector quantization (VQ) was proposed by Chang and Wu [19]. In their scheme, Jo and Kim's [20] watermarking was extended with reversibility in which two extra codebooks were generated. The relationship between the codewords in these codebooks was explored to embed the secret data in the VQ indices. The original VQ indices were recovered by checking the proportion of the codewords in two codebooks.

A data hiding based on side-match vector quantization (SMVQ) was proposed by Chang et al. [21] in 2006. The encoded codeword of the SMVQ scheme is explored to carry the secret message. If the embedded secret bit is equal to 0, the closest codeword by SMVQ is encoded. Otherwise, the approximation of the first closest codeword and the second closest codeword is computed to replace the closest codeword.

Data hiding with reversibility has the advantage of the recovery of the original medium but its hiding capacity is restricted. To obtain reversible data hiding with a higher hiding capacity while preserving a good quality for the medical images, a histogram-based scheme using pixel prediction was proposed in this paper. In the proposed scheme, the relationship between neighboring pixels was explored. A linear prediction technique was employed to process the given image. The generated residual image was then employed to embed the secret data. The residual histogram of the values in the residual image was calculated. The residual histogram and the pairs of peak and zero points were searched to embed secret data.

The rest of this paper is organized as follows: In Section 2, a histogram-based data hiding [14] proposed by Ni. et al. is briefly described. The proposed data hiding using the predictive coding technique is introduced in Section 3. In Section 4, the experimental results are given. Finally, some conclusions are made in Section 5.

2. The histogram-based reversible data hiding

In 2006, Ni et al. [14] proposed a histogram-based reversible data hiding scheme. In their scheme, the occurrences of all possible pixel values in the cover image are calculated to generate the image histogram for secret embedding. Some of pixel values from the histogram are selected and modified to carry the secret data. The modified pixel values can be recovered when the embedded data is extracted, such that the reversible data hiding is achieved.

In the embedding procedure, the pair of peak and zero points from the image histogram is first searched. The peak point is the pixel value with maximum occurrences in the histogram. The zero point is the one with zero or minimum occurrences in the histogram. Pixels with their values ranging from the peak point to the zero point have to be modified. By contrast, pixels with values outside the range are not changed.

The rule for pixel modification is based on the location of pixels in the image histogram. Two scenarios are considered. First, 1-bit secret data *sd* is embedded in each pixel *x* that is located in the peak point. If the value of *sd* equals 1, the value of *x* is kept. Otherwise, the value of *x* is adjusted by 1 to a value closer to the zero point. Second, the value of each pixel *x* is between the peak and zero points but those not equal to the peak point is also shifted by 1 closer to the zero point. In this case, no secret data is embedded in pixel *x*. After all pixels in the image histogram are sequentially processed, the stego-image is generated. Finally, the stego-image and the peak and zero points are transmitted to the receiver.

For secret extraction and image recovery procedure, the stego-image and the pair of peak and zero points are required. Two different ways are used to process each pixel in the stego-image. If the value of one pixel *x* is not within the range of the peak point to the zero point, *x* is skipped. Otherwise, each pixel *x* with value within the range is checked. One of the three cases described in the following is used to process *x*. In the first case, if *x* is located in the peak point, 1-bit secret data valued at 1 is extracted and the value of *x* is unchanged. In the second case, if the absolute difference between *x* and the peak point is 1, 1-bit secret data valued at 0 is extracted and the value of *x* is replaced by the value of the peak point. Lastly, the remaining pixels are shifted to close to the peak point by 1 and no secret data is extracted. After that, the embedded secret data is extracted from the stego-image and the original cover image is recovered.

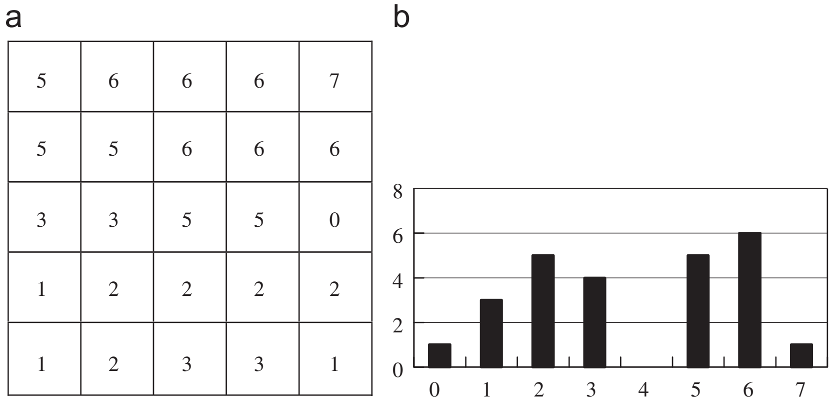
An example of the histogram-based data-hiding scheme is described in the following. One image of 5×5 pixels shown in Fig. 1(a) is taken as the cover image. The corresponding image histogram of the cover image is shown in Fig. 1(b). In this example, the pair of the peak and zero points is searched and the result is (6, 4). From the image histogram, it is found that there are six pixels with value 6. In other words, the maximum hiding capacity of the cover image is 6 bits.

Suppose the secret data $(101100)_2$ is embedded in the cover image, the pixels in coordinates (0,1), (0,2), (0,3), (1,2), (1,3), and (1,4), which are located in the peak point, are selected to carry the secret data. In the embedding procedure, the values of the pixels in coordinates (0,1), (0,3), (1,2) are not modified because 1-bit secret data valued at 1 is embedded in them. At the same time, the values of the pixels in coordinates (0,2), (1,3), (1,4) are adjusted from 6 to 5. The values of the pixels in coordinates (0,0), (1,0), (1,1), (2,2), and (2,3), that are within the range from the peak point to the minimum point are adjusted from 5 to 4. Pixels with their values outside the range are skipped. After that, several pixels are modified and the secret data with 6 bits are embedded. The stego-image is shown in Fig. 2(a).

Further, to extract the secret data and to recover the cover image, the stego-image and the pair (6,4) of peak and zero points are needed. Each pixel in the stego-image is sequentially checked in the order of left-to-right and top-to-bottom. If one pixel valued at 6 is encountered, 1-bit secret data valued at 1 is extracted and the pixel value is unchanged. If one pixel valued 5 is encountered, 1-bit secret data valued at 0 is extracted and the pixel value is replaced by 6. If one pixel valued at 4 is examined, its value is adjusted from 4 to 5 and no secret data is extracted. Finally, the secret data $(101100)_2$ is extracted and the original cover image shown in Fig. 2(b) is reconstructed. The recovered image is the same as that of the original.

The hiding capacity of the histogram-based data hiding equals the number of pixels in the peak point. The larger the number of pixels in the peak point, the higher the hiding capacity. To increase the hiding capacity, more of the peak and zero pairs can be used. Sometimes, it is difficult to find out more pairs of peak and zero points because the zero points are not searched. The minimum number of pixels is usually selected as the zero point. To achieve the reversibility requirements, the location of the pixels in the minimum point must be recorded and embedded. That is the overhead. The size of the overhead may be larger than that of the increased hiding capacity. In this case, the maximum capacity is determined.

The stego-image is quite similar to the original cover in this scheme. This is because only pixels with their values within the range from the peak point to the zero point are



5	6	6	6	7
5	5	6	6	6
3	3	5	5	0
1	2	2	2	2
1	2	3	3	1

Fig. 1. Example of the histogram-based data hiding: (a) cover image and (b) image histogram.

a

4	6	5	6	7
4	4	6	5	5
3	3	4	4	0
1	2	2	2	2
1	2	3	3	1

b

5	6	6	6	7
5	5	6	6	6
3	3	5	5	0
1	2	2	2	2
1	2	3	3	1

Fig. 2. Example of the histogram-based data hiding: (a) stego-image and (b) recovered image.

modified. In addition, the modification of the pixel value is less than or equal to 1. Quite a few pixels with their values outside the range are not modified.

3. The proposed scheme

The proposed scheme explores the neighboring similarity of pixels in the medical image to improve the histogram-based reversible data hiding [14]. The goal of the proposed scheme is to provide a higher hiding capacity while keeping the good quality of the stego-image.

To enlarge the hiding capacity of the histogram-based scheme, the linear prediction technique is employed to process the cover image. Here, the image pixels in the cover image are predicted form the residual image. Secret data are then embedded in the residual image by using a modified histogram-based approach. The proposed scheme consists of two procedures: the secret embedding procedure and the secret extraction and image recovery procedure. An overview of the proposed secret embedding, and secret extraction and image recovery procedures are shown in Figs. 3 and 4, respectively. In addition, a mechanism that can be used to improve the hiding capacity of the proposed scheme is introduced.

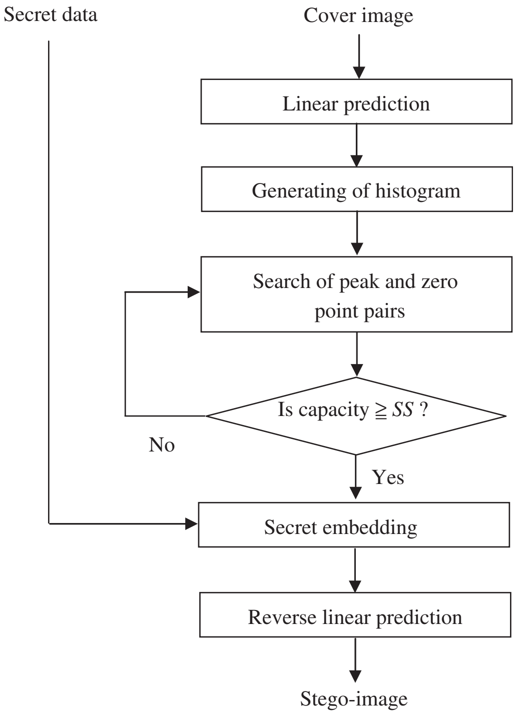


Fig. 3. Flowchart of the proposed embedding procedure.

3.1. The embedding procedure

The similarity between neighboring pixels is explored in the proposed scheme to increase the hiding capacity and to preserve the image quality. Generally, the nature image preserves a stronger similarity between neighboring pixels. According to the histogram-based data hiding, the more dramatically the amplitude for a given histogram changes, the more the hiding capacity does [14]. The linear prediction technique is then employed to achieve the goal.

To explore the similarity between neighboring pixels, the cover image is first divided into blocks of $n \times n$ pixels. First, one pixel in the block is selected as the basic pixel for prediction. Here, the center pixel in the block is selected as the basic pixel. All pixels in the block are processed by the linear prediction technique to generate the prediction errors, also called the residual values. By simply calculating the difference between the basic pixel and each pixel, the prediction error is determined. Each block is sequentially processed in the same manner. After processing all blocks, the residual image is generated. The size of the residual image is the same as the cover image.

Next, the histogram of the residual image is generated. Not all values in the residual image are employed to generate the histogram. After finding the occurrences of residual values that correspond to these non-basic pixels in the cover image, the residual histogram is generated.

The residual histogram can be divided into two parts: non-negative histogram (NNH) and negative histogram (NH). Both NNH and NH change their amplitudes dramatically. This is because the distribution of the values in the residual image is more compact than that of in the original cover image. In addition, there are more zero points in the residual histogram.

After the residual histogram is generated, the secret data are embedded in the residual values of the residual image. Remember, in [14] the secret data are embedded in the pixels in the peak points of the histogram. The same approach is employed in the proposed embedding procedure to embed the secret data. In other words, enough pairs of peak and zero points need to be searched so that the secret data can be totally embedded in the residual image.

Let *SS* denote the size of the secret data to be embedded. First, the pairs of peak and zero points in both NNH and NH are searched. If the maximum hiding capacity derived from NNH and NH is greater than or equal to *SS*, it indicates that there is enough space to embed the secret data. Otherwise, more pairs of peak and zero points in NNH and NH are to be searched until the provided hiding capacity is greater than or equal to *SS*.

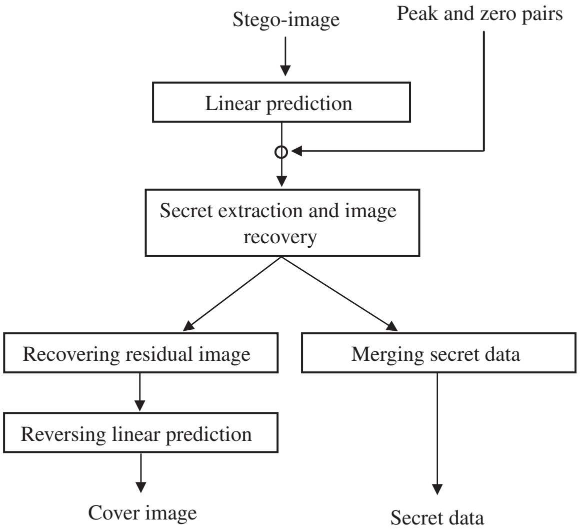

Stego-image
Peak and zero pairs
Linear prediction
Secret extraction and image recovery
Recovering residual image
Merging secret data
Reversing linear prediction
Cover image
Secret data

Fig. 4. Flowchart of the proposed extraction and recovery procedure.

Each residual value in the peak point is employed to carry 1-bit secret data *sd*. One of two possible cases is found for such residual value. If the value of *sd* equals 1, no change is needed for the residual value. Otherwise, the residual value is shifted closer to the value of the zero point by 1. The remaining residual value ranges between the peak and zero points are adjusted to 1 to closer to the zero point. No modification is done for these residual values that are outside the peak and zero pairs. The modification for secret embedding is employed to both NNH and NH.

After the secret data is embedded in the residual image, the residual stego-image is generated. By performing the reverse linear prediction on the residual stego-image, the stego-image of the proposed scheme is obtained.

To avoid the error propagation problem of the reverse linear prediction, the residual values corresponding to the basic pixels in the cover image are not included in calculating the residual histogram. In other words, $(n\times n{-}1)$ residual values are used in each block of $n\times n$ pixels in the cover image. In addition, to provide a good image quality for the stego-image, the absolute distance between the original residual value and its modified values is at most 1. Therefore, the absolute distance between one pixel in the cover image and its corresponding pixel in the stego-image is also at most 1.

An example of the proposed embedding procedure is described in the following. One image of 5×5 pixels shown in Fig. 1(a) is taken as the cover image. Here, the cover image can be viewed as a block of 5×5 pixels. The pixel located in coordinate (2,2) is taken as the basic pixel for this block. The value of the basic pixel is 5. After the linear prediction technique is executed, the residual image, as shown in Fig. 5(a), is generated. Figs. 6(a) and (b) list the NH and NNH of this example, respectively. Note that there are a total of 24 values in the residual histogram except for the basic pixel.

By comparing the histograms shown in Figs. 1 and 6, it is clearly seen that the distribution in the residual histogram is more compact than in the original image histogram. Besides, more zero points are found in NH and NNH. These results imply that the residual image may provide a large hiding capacity when the same embedding rule is used.

Further, two pairs (1, 3) and (−3, −1) of the peak and zero points are searched from the NNH and NH,

a

0	1	1	1	2
0	0	1	1	1
-2	-2	5	0	-5
-4	-3	-3	-3	-3
-4	-3	-2	-2	-4

b

0	1	2	1	3
0	0	1	2	2
-1	-1	5	0	-5
-4	-3	-2	-3	-2
-4	-3	-1	-1	-4

c

5	6	7	6	8
5	5	6	7	7
4	4	5	5	0
1	2	3	2	3
1	2	4	4	1

Fig. 5. Example of the proposed data embedding procedure: (a) the residual image, (b) residual stego-image and (c) the stego-image.

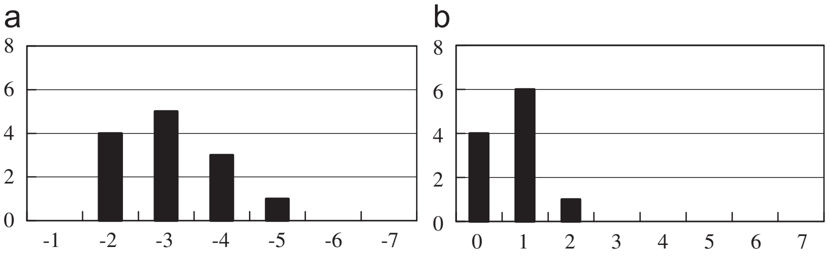


Fig. 6. Example of the residual histogram: (a) the negative histogram NH and (b) the non-negative histogram NNH.

respectively. A total of 7 positive values with their coordinates from (0,1) to (0,4) and from (2,2) to (2,4) have to be modified. Meanwhile, negative values with their coordination from (3,1) to (3,4) and from (4,1) to (4,3) and from (2,0) to (2,1) have to be modified. Of these values, only the values that are equal to peak point can carry the secret bits. Suppose the secret data $(10110010101)_2$ is embedded in the residual image, the residual stego-image of the proposed scheme is shown in Fig. 5(b). Finally, the reverse linear prediction is employed on the residual stego-image to generate the stego-image as shown in Fig. 5(c). From that, the secret data is embedded and a stego-image with less degradation is generated.

However, underflow and overflow of pixel values may also be occurred in the proposed scheme. For example, the original pixel valued at 0 and 255 may be modified to -1 and 256, respectively. To solve this problem, a simple pre-processing work is designed. In pre-processing stage, a zero point that is close to pixel valued at 0 is searched. All pixels less than the selected zero point shift to zero point by one. Similarly, another zero point closer to pixel value of 255 is searched and all pixel greater than this zero point shift to this point by one. From that, both pixel valued at 0 and 255 are removed and underflow/overflow will not occur.

For example, two zero points 5 and 250 are searched from the original image. All pixels with values from 0 to 4 shift to 5 by one and pixel values from 255 to 251 shift to 250 by one. In the recovery procedure, pixel values from 1 to 5 shift to 0 point by one. Also, pixel values from 250 to 254 shift to pixel 250 by one. By doing so, the under/overflow caused by pixels 0 and 255 is eliminated and the image is recovered. However, in the worst case, if the zero point in the original image cannot be searched, the overhead information, which the locations of 0 and 255 must be recorded and embedded, is generated.

3.2. *The extraction and recovery procedure*

The flowchart of the proposed extraction and recovery procedure is depicted in Fig. 4. When the stego-image and the pairs of peak and zero points are ready, the procedure can be started. First, the linear prediction technique used in the embedding procedure is applied again to the stego-image. Then, the residual stego-image is obtained. The pixel of the residual stego-image is examined to extract the embedded secret data and to recover the original image.

This procedure is similar to that of the original histogram-based extraction procedure. Two different ways are considered. If pixel x of the residual stego-image is not within the peak and zero points, this pixel is skipped and the pixel value remains for image reconstruction. Otherwise, three cases are discussed. In the first case, if x is in the peak point, 1-bit secret data valued at 1 is extracted and the value of x is unchanged. In the second case, if the absolute difference between x and the peak point is 1, 1-bit secret data value 0 is extracted and the value of x is replaced by the value of the peak point. Lastly, the remaining pixels are shifted close to peak point by 1 and no secret data is extracted. After that, the embedded secret data is extracted from the stego-image. The original image can be recovered by performing reverse linear prediction to the reconstructed stego-image.

The example shown in Fig. 5 is used again to describe the proposed extraction and recovery procedure. The received stego-image is shown in Fig. 5(c) and two peak and zero pairs for NNH and NH are (1, 3) and (-3, -1), respectively. The residual stego-image is shown in Fig. 5(b).

If the pixel value equals the peak points (1 or -3), the secret message bit value of 1 is extracted. The pixel value is preserved in the image recovery processing. If the absolute difference between the pixel and the peak point is one (like 2 or -2), a bit secret message value of 0 is extracted. And then, the pixel value is replaced with the peak point for the image recovery (from 2 to 1 and from -2 to -3). The other pixels within the peak and zero pairs (3 and -1) are shifted to peak points by one (from 3 to 2 and from -1 to -2) and no secret message is extracted. The remaining pixels out of the peak and zero points are skipped. After that, the embedded secret data $(10110010101)_2$ is extracted. The reconstructed residual image is the same as that shown in Fig. 5(a). The recovered original image is shown in Fig. 1(a).

3.3. *Improvement of hiding capacity*

An optional mechanism to enlarge the hiding capacity is introduced. In the proposed scheme, the maximum hiding capacity is determined according to the number of pixels in the peak points. If a large hiding capacity is required, more peak and zero pairs are used. The overlapping of peak and zero pairs is not permitted in [14]. The crossover between any two pairs is disallowed.

The residual histogram in the proposed method permits the overlapping of pairs of peak and zero points.

Since the residual image preserves a stronger neighboring similarity, it is clear that higher pixel values occur closer to each other. In addition, quite a few residual values with zero occurrences are found. In other words, the distribution of the residual histogram is more compact and a lot of zero points are found. Let k denote the number of pairs to be overlapped. First, k peak values are selected. Then, k zero points are searched to form k pairs of peak and zero points.

An example of two overlapping pairs of peak and zero points are described in the following. In other words, k equals 2 in this example. Here, the NNH shown in Fig. 6(b) is used. First, two peak residual values, 1 and 0, are selected. Then, two zero values, 3 and 4, are selected. Suppose the secret bits $(1010010101)_2$ is to be embedded into the residual image shown in Fig. 5(a), two peak and zero pairs (0,3) and (1,4) with overlapping are employed. In this example, the overlapping area ranges from 1 to 3.

a

1	2	3	2	4
0	1	2	3	2
-2	-2	5	0	-5
-4	-3	-3	-3	-3
-4	-3	-2	-2	-4

b

6	7	8	7	9
5	6	7	8	7
3	3	5	5	0
1	2	2	2	2
1	2	3	3	1

c

0	1	1	1	2
0	0	1	1	1
-2	-2	5	0	-5
-4	-3	-3	-3	-3
-4	-3	-2	-2	-4

Fig. 7. Example of the proposed embedding procedure with peak and zero pairs overlapping: (a) residual stego-image, (b) the stego-image and (c) recovered residual image.

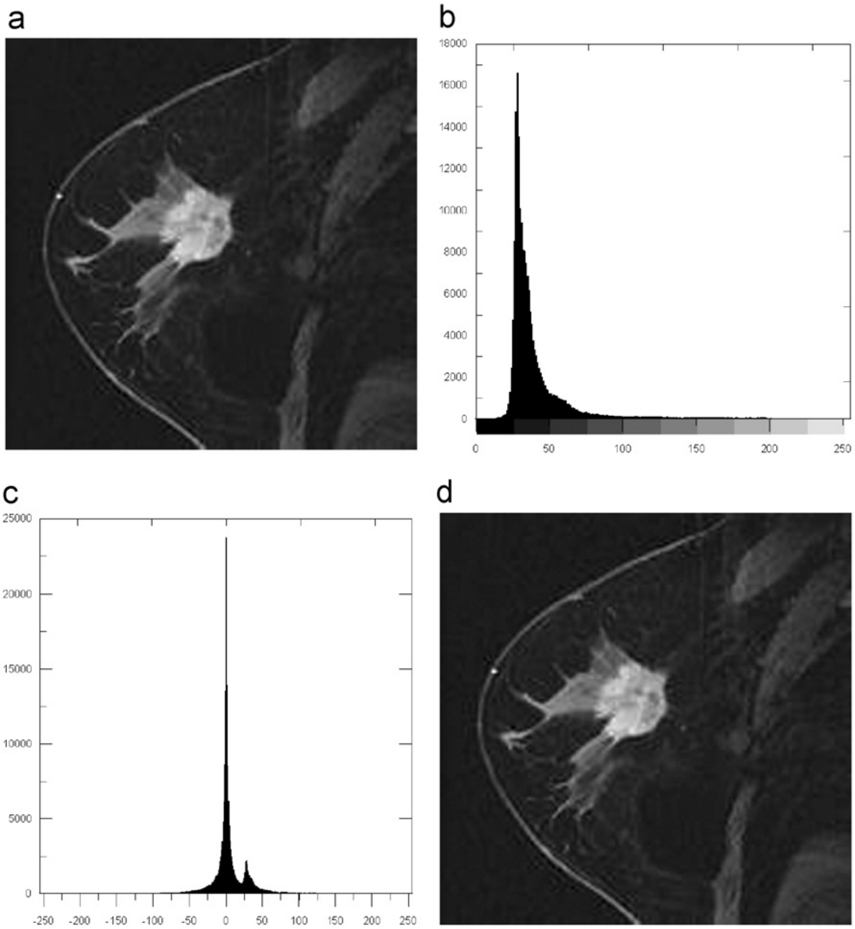


Fig. 8. Testing image "MRI_450_417": (a) original image, (b) original histogram, (c) residual histogram and (d) stego-image.

Three possible rules are used to modify each residual value. First, each residual value, which is not located in the peak value and within the overlapping area, is shifted closer to the zero point with two. Second, the residual values in the peak point within the/an overlapping area is shifted closer to zero point by either one or two according to the embedded secret bit. Third, each residual value that is not in the overlapping area is shifted closer to zero point with one.

According to the searched peak and zero pairs from Fig. 6(b), the values between the peak and zero pairs are modified. First, the non-overlapping peak point value of 0 is modified to 1 if the secret bit 0 is embedded. Accordingly, the overlapping peak point value of 1 is modified to 2 or 3 according to the embedded secret bit 1 or 0. The value of 2 is modified from 2 to 4 in which no secret bit is embedded. The coordinates from (0,0) to (1,4) are modified for secret embedding. The residual stego-image is shown in Fig. 7(a). The reverse linear prediction is performed to generate the stego-image as shown in Fig. 7(b). Regarding the overlapping, the hiding capacity is increased and the degradation of the stego-image is increased because of the maximum pixel difference between the original and modified pixels being equal to 2 in this example.

The secret extraction procedure is similar to the original one except for the processing of the pixels located in the overlapping area. The overlapping area can be known from the received peak and zero pairs (0,3) and (1,4). Each pixel in Fig. 7(a) is checked to extract the embedded secret and to recover the original image. The pixel values of 0 and 1 extract the 1-bit secret value of 1 and 0, respectively, and are recovered by the peak point valued 0. The pixel values of 2 and 3 correspond to the overlapping peak point value of 1, in which a 1-bit of secret valued at 1 and 0 are extracted, respectively. Both pixel values are recovered with the peak point valued 1. On the pixel value of 4, there is no secret data extraction and recovery happens by shifting closer to the peak point by two. The extracted secret data from Fig. 7(a) is $(1010010101)_2$ and the recovery residual image is given in Fig. 7(c) being the same as the original one shown in Fig. 5(a).

4. Experimental results

Several experiments were performed to evaluate the performance of the proposed scheme. Six gray-level medical images were used in the experiments and are

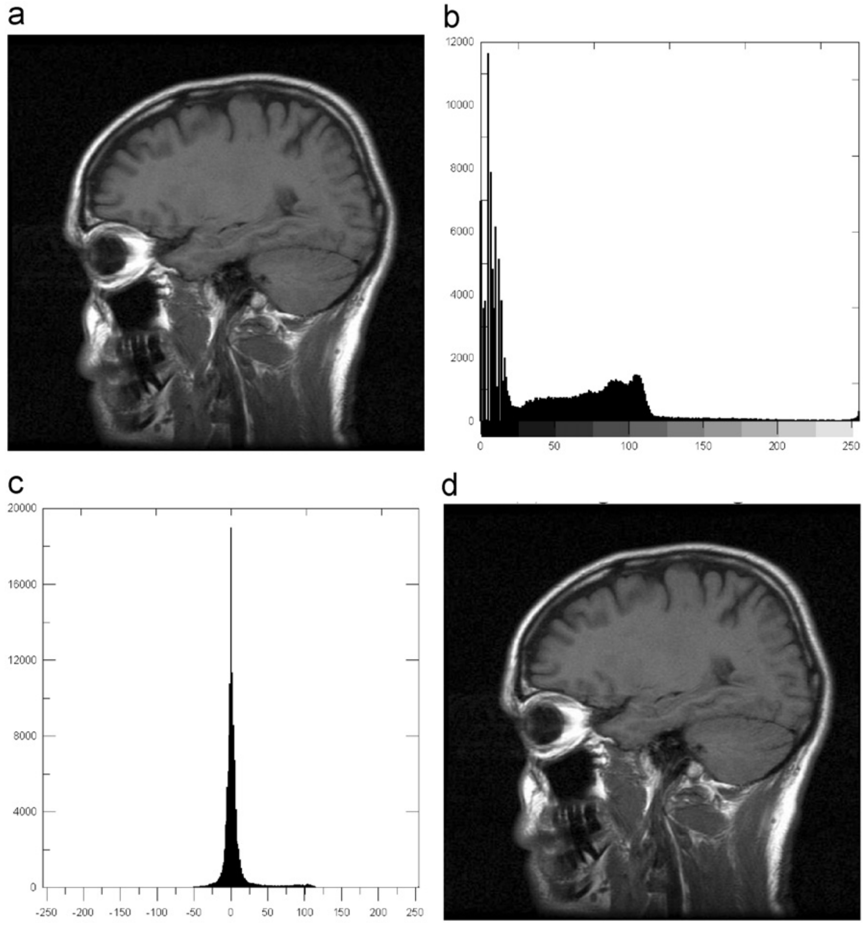


Fig. 9. Testing image "MRI_400_400": (a) original image, (b) original histogram, (c) residual histogram and (d) stego-image.

shown in Figs. 8–13. In the simulations, these test images were first divided into blocks of 3 × 3 pixels. And then, the linear prediction was performed to generate the residual images. In other words, 8 residual values are generated for each 3 × 3 block.

To demonstrate the rearranged image pixel distribution, the histograms of these medical images and the residual images are shown in Figs. 8(b)–13(b) and Figs. 8(c)–13(c), respectively. The histograms generated by the residual images contain one NH and another NNH. In Figs. 8(c)–13(c), it is noted that the pixel distribution in the residual image is more compact and concentrated on a few of pixel values. By comparing the histograms generated by the original images and the residual images, it is clear that the proposed residual histograms change more dramatically in amplitude than the original image. According to Ni et al.'s experiment [14], the histogram with the sharper amplitude has a higher hiding capacity. From the results of Figs. 8(b) and (c), the numbers of pixels in the peak points for the original, NH and NNH histograms are 16,591, 23,723, and 13,539, respectively. The hiding capacity of the residual image is 37,262 bits (23723+13539), which is larger than the original image, providing 16,591 bits. The other examples shown in Figs. 9(c)–13(c) also have the same results.

To further explore the relationship between the hiding capacity and the similarity of neighboring pixels, the hiding capacities with different block sizes are computed. One peak and zero pair are searched from NH and NNH, respectively. The results of the hiding capacity and block sizes are shown in Table 1. In Table 1, it can be seen that the block with 3 × 3 pixels holds a stronger neighboring similarity and provides the largest hiding capacity and the block with 4 × 4 pixels follows. From Table 1, it is noted that the larger the block size, the lower the neighboring similarity and the less the hiding capacity is even though the number of basic blocks is smaller.

To further explore the relationship between the hiding capacity and the similarity of neighboring pixels, the hiding capacities with different block sizes are computed. One peak and zero pair are searched from NH and NNH, respectively. The results of the hiding capacity and block sizes are shown in Table 1. In Table 1, it can be seen that the block with 3 × 3 pixels holds a stronger neighboring similarity and provides the largest hiding capacity and the block with 4 × 4 pixels follows. From Table 1, it is noted

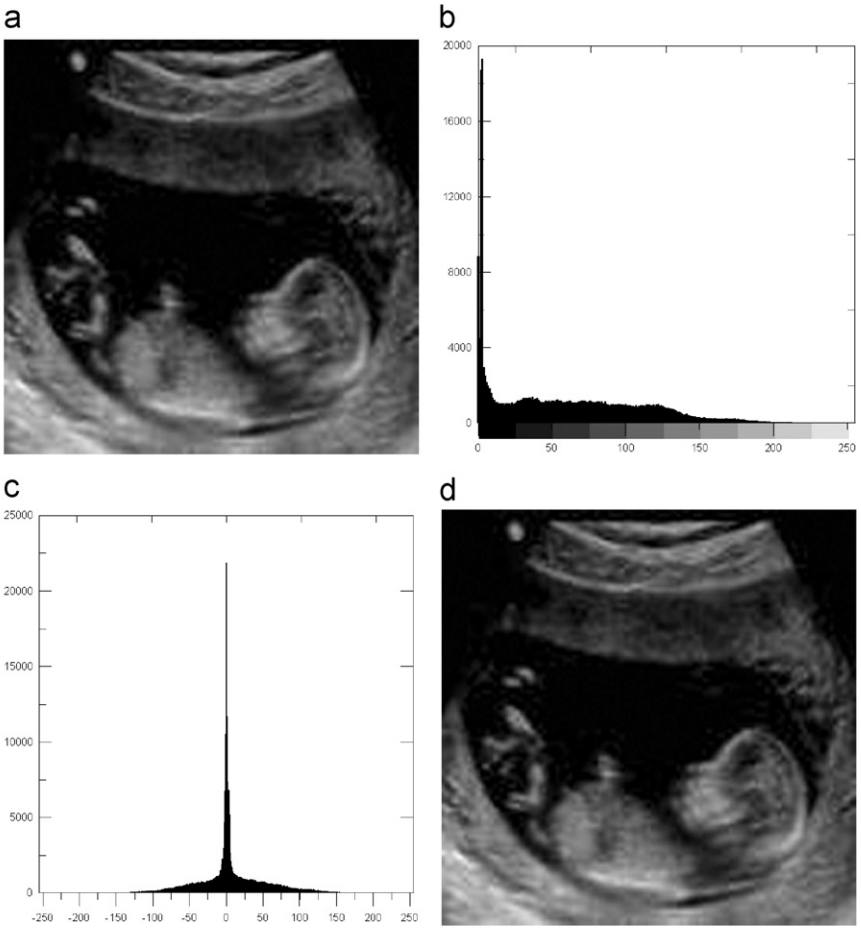


Fig. 10. Testing image "Ultra_508_424": (a) original image, (b) original histogram, (c) residual histogram and (d) stego-image.

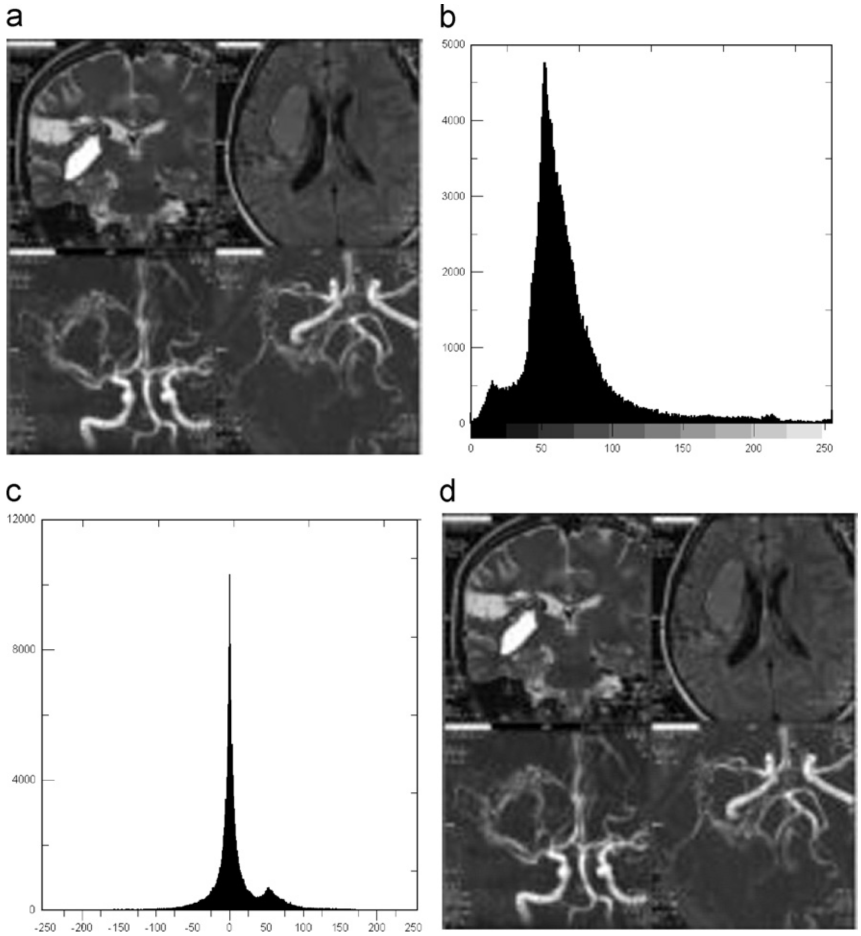


Fig. 11. Testing image "CT_405_399": (a) original image, (b) original histogram, (c) residual histogram and (d) stego-image.

that the larger the block size, the lower the neighboring similarity and the less the hiding capacity is even though the number of basic blocks is smaller.

To evaluate the performance of the proposed method, the hiding capacity and the stego-image quality are computed. The hiding capacity shown in Table 1 with block size of 3×3 is employed to embed the secret data. The size of the embedded secret data is determined according to the capacity of the supported image. Table 2 shows the experimental results of the hiding capacity and the stego-image quality. From Table 2, it is found that the average of the stego-image quality is greater than 49 dB while the average size of the embedded secret data is more than 42 K bits. This result indicates that the image distortion caused by the proposed embedding procedure is less. The stego-images are given in Figs. 8(d)–13(d). By comparing Figs. 8(a)–13(a) and 8(d)–13(d), it is difficult to distinguish the difference between the original image and the stego-image with the naked eye.

The relationship between the hiding capacity and the stego-image quality of the proposed scheme is further explored. In this experiment, more peak and zero pairs with overlapping were determined. The experimental results are shown in Fig. 14 in which the hiding capacity is presented by bit rate (bpp: bit per pixel). From Fig. 14, it is noted that the quality of stego-image was also preserved at about 41 dB at the embedding bit rate 0.47 bpp. This result shows a large hiding capacity and a good image quality.

To further enlarge the hiding capacity, more of the peak and zero pairs from NH and NNH are searched. In the proposed scheme, the overlapping between peak and zero pairs is permitted and can be determined according to the user requirement. The hiding capacities and the stego-image qualities of the test images with overlapping and non-overlapping peak and zero pairs were shown in Table 3.

From Table 3, the hiding capacities and stego-image qualities of different pairs in non-overlapping are quite close. This is because the distribution of residual values in the residual image is more compact and the number of residual values in the second and third peak points is small. On the other hand, the hiding capacity is enlarged about 25 and 39 K bits when two and three overlapping pairs are employed. Although, the qualities of stego-image are degraded about 3 and 6 dB, but the average stego-image quality is still preserved about 43 dB in three pairs. In summary, the overlapping mechanism enlarged the

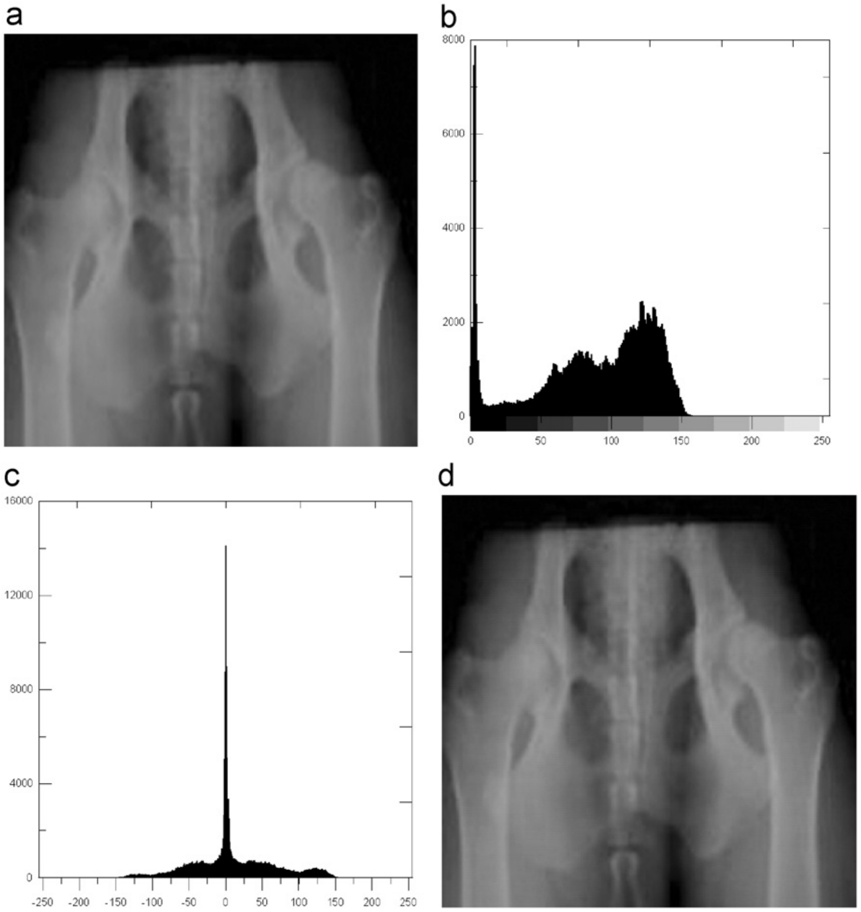


Fig. 12. Testing image “X-ray_480_360”: (a) original image, (b) original histogram, (c) residual histogram and (d) stego-image.

hiding capacity efficiently and a good stego-image is also preserved.

To compare the performance of the histogram-based data hiding scheme [14] and the proposed scheme, results of the hiding capacity and the quality of the stego-image are shown in Table 4. In this experiment, the maximal hiding capacity according to [14] is provided. In Table 4, a better stego-image quality in test images “MRI_400_400” is obtained in Ni et al.’s scheme. This is because a great number of pixels are shifted to avoid overhead in the proposed method. However, on the average results, it is seen that the proposed scheme obtained a better quality of stego-image than the original histogram-based scheme by about 1.5 dB when the same size secret data were embedded. Furthermore, comparing the average hiding capacity shown in Tables 2 and 4, it is noted that the hiding capacity of the proposed scheme is about three times larger than that of the histogram-based data hiding scheme.

In the simulation of the histogram-based scheme [14], different types of testing images including the standard grayscale images, the medical images, the texture images, the aerial images, and the CorelDrew images were used. The main contribution of the histogram-based scheme is that it provides a framework for reversible image hiding based on histogram shifting. The applications of it are not specific. Therefore, the security and the robustness issues are not mentioned.

As we know, the hiding capacity of the non-reversible data hiding scheme is definitely higher than that of the reversible data hiding. Therefore, the target application of one reversible data hiding scheme is not steganography because of the limitation of the hiding capacity. In the proposed scheme, the target application can be in medical video authentication. In Zhao et al.’s video watermarking [22], the watermark is embedded according to the motion vector selection. Motion vector is computed by using prediction algorithm. Accordingly, the proposed method by linear prediction applied to medical video authentication with reversibility is possible. After all, reversible medical video authentication is important to authenticate the originality and to verify the integrity.

To evaluate the robustness of the proposed method, several approaches were explored [21,23]. Since the proposed method is based on LSB, chi-square steganalysis test program is employed [23]. In chi-square steganalysis, the result is presented with a red curve and the distribution of green curve. The red curve closer to one

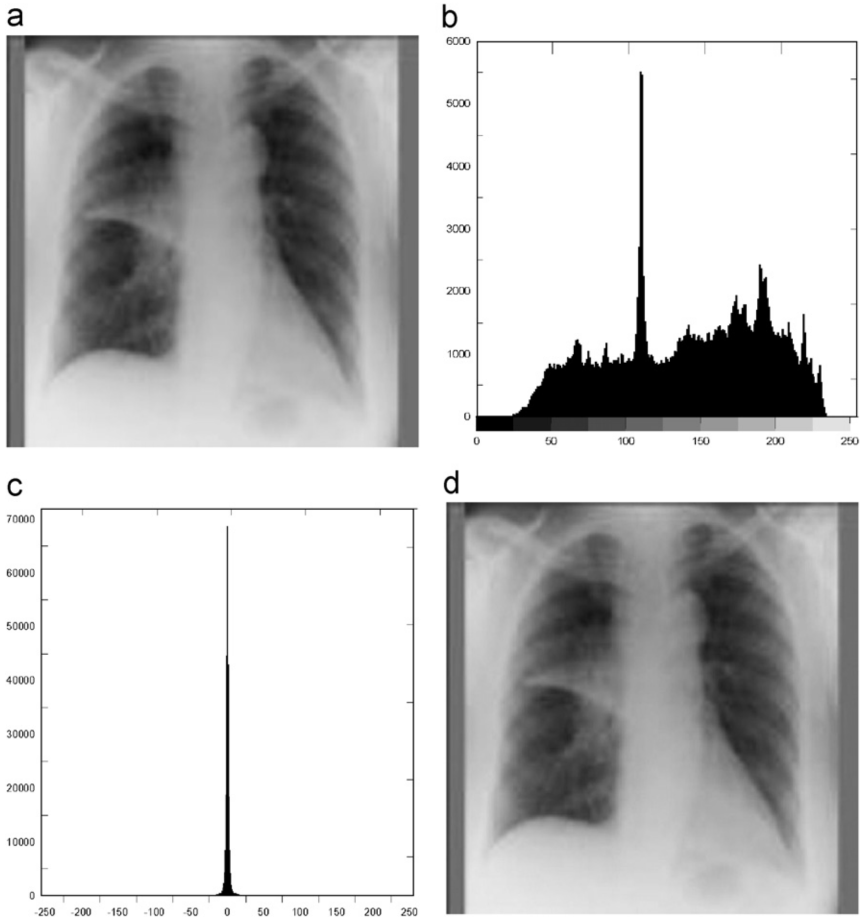


Fig. 13. Testing image "X-ray_512_512": (a) original image, (b) original histogram, (c) residual histogram and (d) stego-image.

Table 1
Hiding capacity (unit: bit) and different block sizes.

Images	Block sizes			
	3 × 3	4 × 4	5 × 5	7 × 7
Mri_450_417	37,262	32,415	29,613	24,732
Mri_400_400	30,622	29,630	28,267	25,593
Ultra_508_424	32,427	26,715	22,624	17,985
CT_405_399	18,399	15,996	14,920	12,520
X-ray_480_360	22,852	19,659	16,435	12,233
X-ray_512_512	113,218	100,743	98,532	84,920
Average	42,463	37,526	35,065	29,664

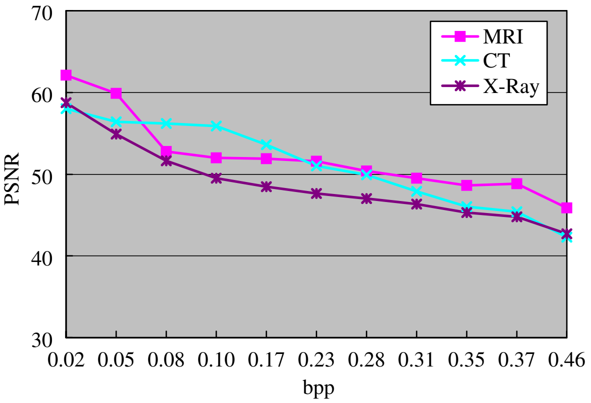


Fig. 14. Relationship between the stego-image quality and the hiding capacities.

indicates a high probability of a random embedded secret message. The green curve is used to imply the average value of the LSB. The distribution of green curve closer to 0.5 also indicates a random secret message is embedded.

In this experiment, the original cover image, the stego-image by random secret embedding and the stego-image by the proposed method were attacked. The results were shown in Fig. 15. In Fig. 15(a), the original image "MRI_400_400" is attacked. Since no secret message is embedded in the original image, so the red curve located zero. In Fig. 15(b), a random secret data is embedded into the LSB of the cover image "MRI_400_400". The red curve closer to one indicates the secret embedding is detected. Also, the distribution of the green curve is near to 0.5, which also implies a random secret data is embedded. In Fig. 15(c), the green curve average of LSBs is variable and the Chi-square red curve is flat and at zero that is similar to the result shown in Fig. 15(a). This result indicates the embedded secret message is undetected.

Another robustness experiment by Stirmark benchmark was performed. The results were showed in Table 5. In Table 5, the strength of the watermark embedding is set to 20 in first column. The noise level is 2 in the second column for noise addition. In median cut simulation, the filter size is 3 × 3. In JPEG compression, the quality factor is set to 80. In last column, the 25% of the stego-image is cropped. From Table 5, it is shown that the error rate of extracted secret data is quite high. This result indicates that the proposed scheme is sensitive to against Stirmark test. The feature of sensitivity is important in digital authentication.

5. Conclusions

In this paper, a reversible data hiding scheme using linear prediction for medical images is presented. The proposed scheme intends to improve the histogram-based data hiding scheme which embeds secret data into the peak points of the image histogram. To achieve a higher hiding capacity, secret data are embedded in the residual images instead of the image histogram. The distribution of the residual values after linear prediction is explored for secret embedding. In addition, by overlapping the pairs of peak and zero points, the hiding capacity of the proposed scheme is further improved.

According to the results, the proposed reversible data hiding scheme provides a higher hiding capacity while achieving better image quality for stego-images. That is because no additional overhead for coordination information is required as in [14]. Besides, the computational cost of the proposed scheme is very small. Since the hiding capacity, quality and sensitivity of the proposed scheme are high, it can be used for medical video authentication. The security of the secret data can be further safeguarded by using encryption/decryption techniques such as AES before it is embedded into the host images.

Table 2
Hiding capacity (unit: bit) and the stego-image quality (by PSNR).

Images	Factors	
	Capacity	Quality
MRIi_450_417	37,262	50.61
MRI_400_400	29,771	51.60
Ultra_508_424	32,427	46.80
CT_405_399	18,399	51.03
X-ray_480_360	22,852	47.66
X-ray_512_512	113,218	49.85
Average	42,322	49.59

Table 4
Capacity (unit: bit) and the image quality (PSNR) of the histogram-based scheme and the proposed scheme.

Images	Methods			
	Ni et al.'s scheme [14]		Proposed scheme	
	Capacity	Quality	Capacity	Quality
MRI_450_417	16,591	50.69	16,592	54.37
MRI_400_400	26,505	56.98	26,505	52.00
Ultra_508_424	19,287	49.92	19,287	47.89
CT_405_399	4,762	51.81	4,762	55.87
X-ray_480_360	7,871	50.32	7,871	49.53
X-ray_512_512	13,002	48.24	13,002	58.05
Average	14,670	51.33	14,670	52.95

Table 3
Hiding capacities (unit: bit) and image qualities (PSNR) with overlapping and non-overlapping peak and zero pairs.

Images	Pairs							
	Two pairs				Three pairs			
	Overlapping		Non-overlapping		Overlapping		Non-overlapping	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
MRI_450_417	59,790	47.88	37,270	50.61	74,475	44.96	37,270	50.61
MRI_400_400	51,408	48.82	29,712	51.60	70,357	45.85	29,714	51.60
Ultra_508_424	49,383	45.36	32,427	46.80	61,334	41.70	32,432	46.80
CT_405_399	32,909	45.43	18,402	51.03	35,499	42.28	18,406	51.03
X-ray_480_360	36,747	46.34	22,854	47.66	44,285	42.69	22,860	47.66
X-ray_512_512	174,870	45.86	113,218	49.85	201,602	44.17	113,218	49.85
Average	67,518	46.62	42,314	49.59	81,259	43.61	42,317	49.59

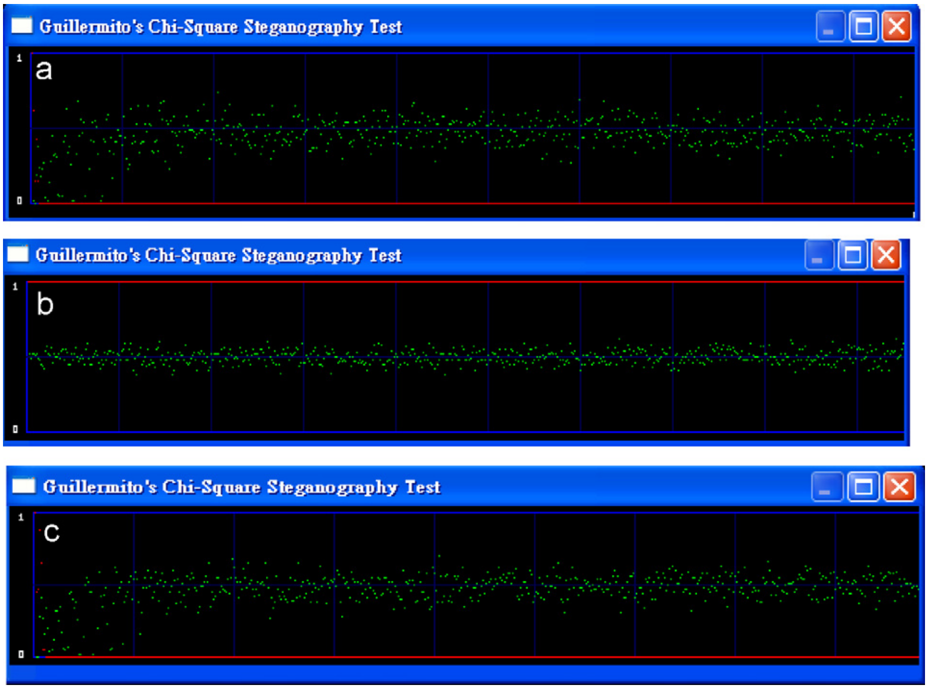

Guillermito's Chi-Square Steganography Test
1
a
0
Guillermito's Chi-Square Steganography Test
1
b
0
Guillermito's Chi-Square Steganography Test
1
c
0

Fig. 15. Test image “MRI_400_400” for Chi-square attack: (a) Chi-square result of original “MRI_400_400”, (b) Chi-square result of stego-image “MRI_400_400” by random secret embedding in 1-LSB of each pixel and (c) Chi-square result of stego-image by the proposed method.

Table 5
Error rate (by %) of extracted secret data from Stirmark benchmark Test.

Iamges	Attacks				
	Strength	Noise	MedianCut	JPEG	Cropping
MRI_450_417	37.53	50.12	49.75	50.29	50.03
MRI_400_400	45.85	49.48	48.97	49.80	49.08
Ultra_508_424	37.27	49.80	50.50	49.87	50.24
CT_405_399	37.99	49.36	49.52	48.86	49.86
X-ray_480_360	40.70	50.05	49.77	49.73	49.92
X-ray_512_512	33.01	49.71	49.18	49.51	49.12
Average	38.73	49.75	49.62	49.68	49.71

Acknowledgment

This research was supported by the National Science Council, Taipei, R.O.C. under contract NSC 95-2221-E-126-008-MY2.

References

[1] Q. Cheng, T.S. Huang, An additive approach to transform-domain information hiding and optimum detection structure, IEEE Transactions on Multimedia 3 (3) (2001) 273–284.

[2] D. Artz, Digital steganography: hiding data within data, IEEE Internet Computing 5 (3) (2001) 75–80.

[3] C.I. Podilchuk, E.J. Delp, Digital watermarking: algorithms and applications, IEEE Signal Processing Magazine 18 (4) (2001) 33–46.

[4] R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683.

[5] J. Spaulding, H. Noda, M.N. Shirazi, E. Kawaguchi, BPCS steganography using EZW lossy compressed images, Pattern Recognition Letters 23 (13) (2002) 1579–1587.

[6] W.C. Du, W.J. Hsu, Adaptive data hiding based on VQ compressed images, IEE Proceedings of Vision, Image and Signal Processing 150 (4) (2003) 233–238.

[7] N. Yu, L. L. Cao, W. Fang, X. L. Li, Practical analysis of watermarking capacity, in: Proceedings of IEEE International Conference on Communication Technology, 2003, pp. 1872–1877.

[8] P. Tsai, Y.C. Hu, C.C. Chang, A progressive secret reveal system based on SPIHT image transmission, Signal Processing: Image Communication 19 (3) (2004) 285–297.

[9] C.C. Chang, Y.H. Yu, Y.C. Hu, Hiding secret data in images via predictive coding, Pattern Recognition 38 (5) (2005) 691–705.

[10] Y.C. Hu, High capacity image hiding scheme based on vector quantization, Pattern Recognition 39 (9) (2006) 1715–1724.

[11] C. Deng, X.B. Gao, D.C. Tao, X.L. Li, Digital watermarking in image affine co-variant regions, in: Proceedings of IEEE International Conference on Machine Learning and Cybernetics, HK, 2007, pp. 2125–2130.

[12] M.U. Celik, G. Sharma, A.M. Tekalp, Reversible data hiding, in: Proceedings of IEEE International Conference on Image Processing, Rochester, NY, 2002, pp. 157–160.

[13] J. Tian, Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (2003) 890–896.

[14] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Transactions on Circuits and Systems for Video Technology 16 (3) (2006) 354–361.

[15] C.L. Tsai, H.F. Chiang, K.C. Fan, C.D. Chung, Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism, Pattern Recognition 38 (11) (2005) 1993–2006.

[16] J. Fridrich, M. Goljan, R. Du, Invertible Authentication, in: Proceedings of SPIE Security Watermarking Multimedia Contents, San Jose, CA, January 2001, pp. 197–208.

[17] G. Xuan, J. Zhu, J. Chen, Y.Q. Shi, Z. Ni, W. Su, Distortionless data hiding based on integer wavelet transform, Electronics Letters 38 (25) (2002) 1646–1648.

[18] L. Kamstra, H.J.A.M. Heijmans, Reversible data embedding into images using wavelet techniques and sorting, IEEE Transactions on Image Processing 4 (12) (2005) 2082–2090.

[19] C. C. Chang, W. C. Wu, A reversible information hiding scheme based on vector quantization, in: Proceedings of Knowledge-Based Intelligent Information and Engineering Systems (KES 05), Melbourne, Australia, September 2005, pp. 1101–1107.

[20] M. Jo, H.D. Kim, A digital image watermarking scheme based on vector quantization, IEICE Transactions on Information and Systems 9 (3) (2002) 1054–1056.

[21] C.C. Chang, W.L. Tai, C.C. Lin, A reversible data hiding scheme based on side-match vector quantization, IEEE Transactions on Circuits and Systems for Video Technology 16 (10) (2006) 1301–1308.

[22] Z. Zhao, N. H. Yu, X. L. Li, A novel video watermarking scheme in compressed domain based on fast motion estimation, in: Proceedings of IEEE International Conference on Communication Technology, vol. 2, 2003, pp. 1878–1882.

[23] Guillermito, Chi-square Steganography 〈http://www.guillermito2.net/stegano/tools/index.html〉.