An Image Authentication Method for Secure Internet-Based Communication in Human-Centric Computing

Yung-Yao Chen[1], Chih-Hsien Hsia[2], Hsiang-Yun Kao[3], You-An Wang[3], Yu-Chen Hu[4]

[1] Dept. Electronic and Computer Engineering, National Taiwan U. Science and Technology, Taiwan

[2] Dept. Computer Science and Information Eng., National Ilan University, Taiwan

[3] Grad. Inst. of Automation Technology, National Taipei Tech. University, Taiwan

[4] Dept. Computer Science and Information Management, Providence University, Taiwan

yungyaochen@mail.ntust.edu.tw, chhsia625@gmail.com, t106618033@ntut.edu.tw, t107618016@ntut.edu.tw, ychu@pu.edu.tw

Abstract

With the rapid development of computing technologies, human-centered computing (HCC) has become an emerging multidisciplinary area which integrates ubiquitous computing, wearable computing, and so on. When large amounts of information has to be mutually analyzed, HCC aims to bridge the gap between people and computing systems. However, ensuring a secure transmission becomes challenging in HCC because malicious hackers tend to tamper with the Internet data. The massive amount of counterfeited or tampered data on the Internet damage data trustworthiness and impede the progress of HCC. To address this problem, this study presented an image authentication method based on the residual histogram shifting technique. In this technique, an image histogram is generated using block-based processing. Then, the histogram is modified to achieve a high embedding capacity. By manipulating the image histogram, secret or authentication codes can be embedded in the image itself to prevent private information from being tampered without consent. The quality of the obtained stego image is preserved because the shifting of the histogram is controlled to be within the minimum degree. Moreover, the proposed image authentication method is a reversible scheme which can recover the original host image from the stego image. From the experimental results, it reveals that the proposed method provides larger hiding capacity than the state-of-the-art methods, while maintaining pleasing image qualities of the embedded images.

Keywords: Image authentication, Secure internet-based communication, Human-centric computing, Data hiding, Steganography

1 Introduction

Human-centered computing (HCC) can be considered as a combination of different disciplines, such as information science and human-computer interaction. Currently, the considerable progress in artificial intelligence (AI) technologies, such as deep learning and convolution neural network (CNN), has increased the processing efficiency of big data technologies significantly. For example, Yin et al. proposed a mobile marketing recommendation method [1] that considers the user's location. By using an open dataset that contains the various behaviors of 10 million user, the method presented in [1] presents an accuracy rate improvement of nearly 10% in both accuracy and recall rates. Another HCC example is the combination of medical diagnosis and AI to create an intelligent healthcare system [2]. Learning from tons of medical images using AI, modern technology is able to provide precise and trustworthy diagnosis. However, personal privacy protection should be highly valued, and the balance between utility and security of these medical data should be handled carefully [3-6].

On the other hand, a highly developed Internet technology not only changes the living habits of people but also exerts a greater concern of privacy protection on the Internet. Image data hiding or steganography is one of the most effective technologies that can prevent privacy leakage. It can be used to hide personal or government agencies' secret data into images for transmission. Even if stego images are obtained by a third party, the secret data cannot be extracted and intercepted. Therefore, different image data hiding technologies are constantly innovated to prevent confidential information from being illegally acquired and is used in applications that require a high- or low-level secure transmission.

Image data hiding can be divided into two categories: reversible and irreversible. In irreversible data hiding methods [7-11], the original image cannot be recovered after hiding data, but the advantage is that it can hide data without restore additional information. Among them, least significant bit (LSB), pixel value

differencing (PVD) and exploiting modification direction (EMD) might be three of the most common techniques used to achieve irreversible data hiding. The concept of LSB, PVD and EMD can be found be in most papers involved irreversible data hiding more or less. The method of [7], proposed a data hiding method that can embed three secret bits into the group of three pixels by modification the each pixel at most +1 or -1. The method of [8] first mapped the image into 1D pixels sequence by a Hilbert curve. Then, the 1D sequence is divided into non-overlapping units with two consecutive pixels, and the secret bits are embedded by exploiting the pixel value difference. In [9], a Generalized EMD (GEMD) was proposed. By dividing the cover pixels into different sub-groups and embedding data in individual sub-groups, GEMD significantly increases the data capacity of the traditional EMD method.

In reversible data hiding (RDH) methods [12-16], they normally emphasize that when the image is transferred and received at the receiver end, the original image can be completely recovered without any loss of information. The types of images which usually involve RDH techniques include medical images, personal (private) images, confidential military images, and so on. The method of [12] utilized sparse representation scheme in patch-level to embed data by exploring the neighboring pixels correlation. A learned dictionary is also embedded into the cover image to decode the leading residual errors. The method of [13] proposed a data hiding method which estimates the image block complexity by evaluating the locations of neighboring pixels. Therefore, the extracted-bit error rate is decreased, especially when the block size is large. The method of [14] proposed a RDH method for the Joint Photographic Experts Group (JPEG) compressed image, where the zero discrete cosine transform (DCT) coefficients are unchanged, but those non-zero DCT coefficients are modified for data-embedding.

In RDH methods, histogram modification or histogram shifting is one of the most common strategies to hide data recently [17-21]. It hides data into the cover image by utilizing the characteristic of peak point and zero point of an image histogram. The method of [17] presented a histogram shifting method, which combines the linear pixel-error prediction scheme and the block truncation coding (BTC) technology to carry out the residual histogram shifting in compressed images. The method of [18] presented a RDH method, which embeds data into a cover image by selecting two expansion bins in each histogram and then performing a multiple histograms modification. The method of [19] presented a RDH method with an additional advantage of contrast enhancement by utilizing histogram shifting and pixel value ordering schemes. Moreover, the data capacity is increased, and the visual distortion is reduced. The method of [20]

applied the histogram shifting technique in encrypted images, where the image histogram is first expanded by utilizing the homomorphic multiplication using public key cryptosystem. The method of [21] presented a RDH method for JPEG images, which first selects the high-frequency coefficients by analyzing the histogram distribution and embeds the secret data on those high-frequency coefficients. There are some techniques which can further improve the security of data-hiding. For example, chaotic system is one of the ways to generate pseudo random numbers, which can be applied to weak signal detection as well [22].

In this study, we aim to improve a steganography technique that is based on the histogram shifting (HS) technique. In general, when more than one peak point is utilized, the number of pixel occurrences at the peak points (i.e., the total embedding capacity) cannot be effectively utilized, the number of pixel occurrences at the peak points cannot be effectively increased. This effect occurs because of some restrictions in the selection phase of multiple boundary point pairs. To address this problem, this study presented novel rules for multiple pair selection and the corresponding data-embedding procedure.

2 Related Works

In [23], Ni et al. proposed a reversible data hiding method based on the HS technique. The histogram of any input grayscale image is first generated, which implies that the occurrence frequencies of the pixels from [0, 255] are calculated. In the histogram, the search rule of boundary points is defined as follows:

$$\begin{cases} PP = \text{intensity value with highest occurence} \\ ZP = \text{intensity value with no occurence} \end{cases} ., \quad (1)$$

Before the secret data is embedded, a pair of PP and ZP should be determined. There might be multiple intensity values which have the same highest occurrences. In this case, any of them can be selected as PP. Moreover, there might be multiple intensity values that have no occurrences. In this case, the ZP that is the closest to the determined PP is selected. To achieve the minimum image distortion for maintaining image quality, only the pixels within the range of [PP, ZP] (or [ZP, PP]) are moved.

As shown in Figure 1, to create space for data that has to be embedded (the to-be-embedded data), the histogram is modified as follows:

$$x' = \begin{cases} x + 1, & \text{if } x \in (PP, ZP) \\ x, & \text{otherwise} \end{cases} \quad (\text{case of } PP < ZP) \quad (2)$$

and

$$x' = \begin{cases} x - 1, & \text{if } x \in (ZP, PP) \\ x, & \text{otherwise} \end{cases} \quad (\text{case of } PP > ZP), \quad (3)$$

(a)

(b)
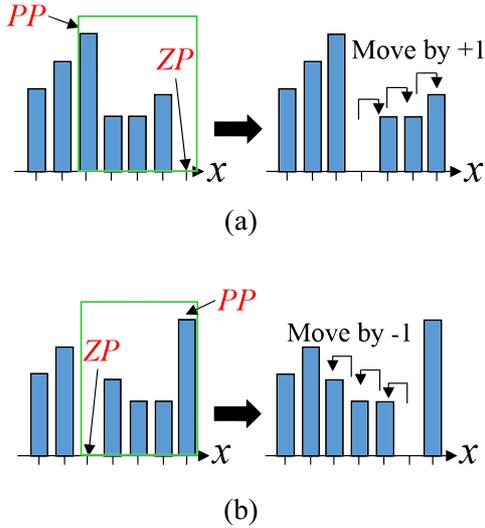
Figure 1. Histogram modification when (a) $ZP > PP$, and (b) $ZP < PP$

The range between the two boundary points, PP and ZP, is defined as the data-embedding region. The embedding capacity of the data-embedding region is determined using the number of pixels np in PP. Apparently, finding more non-overlapping regions leads to higher total embedding capacity in the output stego image. However, the required extra storage of recording the pairs of the peak points and zero points is more. In [24], Tsai et al. extended the study presented in [23], in which the predictive coding scheme is applied to generate a residual histogram and to enlarge the data capacity. The neighboring similarity is utilized to increase the possibility of obtaining a larger np value.
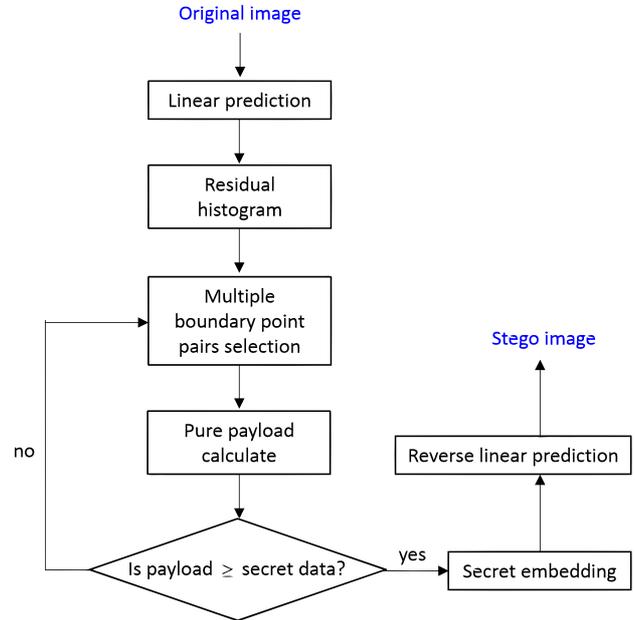
3 Proposed Method

3.1 Cascading Linear Prediction

Figure 2 shows the overall framework of the proposed method. By generalizing our previous work [25], this study aims to present a high-capacity HS-based data hiding method by simultaneously utilizing two aspects: 1) generating a more concentrated histogram; and 2) designing a more flexible embedding rule. First, the input image is divided into non-overlapped square blocks with a size of n. The reference position of each block is defined as follows:

$$\text{Ref. Position} = \lfloor n/2 \rfloor \times n + \lceil n/2 \rceil \ (n \geq 3), \quad (4)$$

where the symbol $\lfloor \; \rfloor$ indicates the rounded-down nearest integer and the symbol $\lceil \; \rceil$ indicates the rounded-up nearest integer. As shown in Figure 3(a), Pi represents the i-th pixel value, where the subscript i indicates the pixel position arranged left-to-right and top-to-down orderly. To maximize the neighboring similarity, each image block can be further partitioned

into non-overlapped hierarchies centered at the reference position. The cascading linear prediction scheme is performed so that no matter how big the block size is, only the 8-neighboring pixels can be used to generate the residual values.

Figure 2. Overall framework of the proposed method

By using a 6×6 block as an example, there are eight (predicted) residual errors in the first hierarchy, sixteen (predicted) residual errors in the second hierarchy, and eleven (predicted) residual errors in the third hierarchy. It was demonstrated that when the residual errors r_i are calculated, the error prediction technique is performed progressively from the outside to the inside, as presented in Figure 3(b) to Figure 3(d). This implies that the prediction errors in the third hierarchy (Figure 3d) are calculated first, then the prediction errors in the second hierarchy (Figure 3c) are calculated, and finally the errors in the first hierarchy (Figure 3b) are calculated. Conversely, while recovering the original image block, the original pixels values P_i are retrieved progressively from the inside to the outside, i.e., retrieving the pixel values in the first hierarchy positions first. After applying the cascading prediction technique in all image blocks, the residual histogram can be generated by counting the occurrence frequencies of individual residual errors cumulatively.

3.2 Multiple Boundary Point Pairs Selection

Note that due to the property of the prediction errors, each stego image has two residual histograms: one negative histogram and one non-negative histogram. Basically, we can embed data by the same embedding rule in each of them. For simplicity, hereafter we only discuss the case of non-negative residual histogram. In (1), the pair of boundary points refers to one peak point and one zero point, which defines a single specific data-embedding region. If a higher embedding capacity
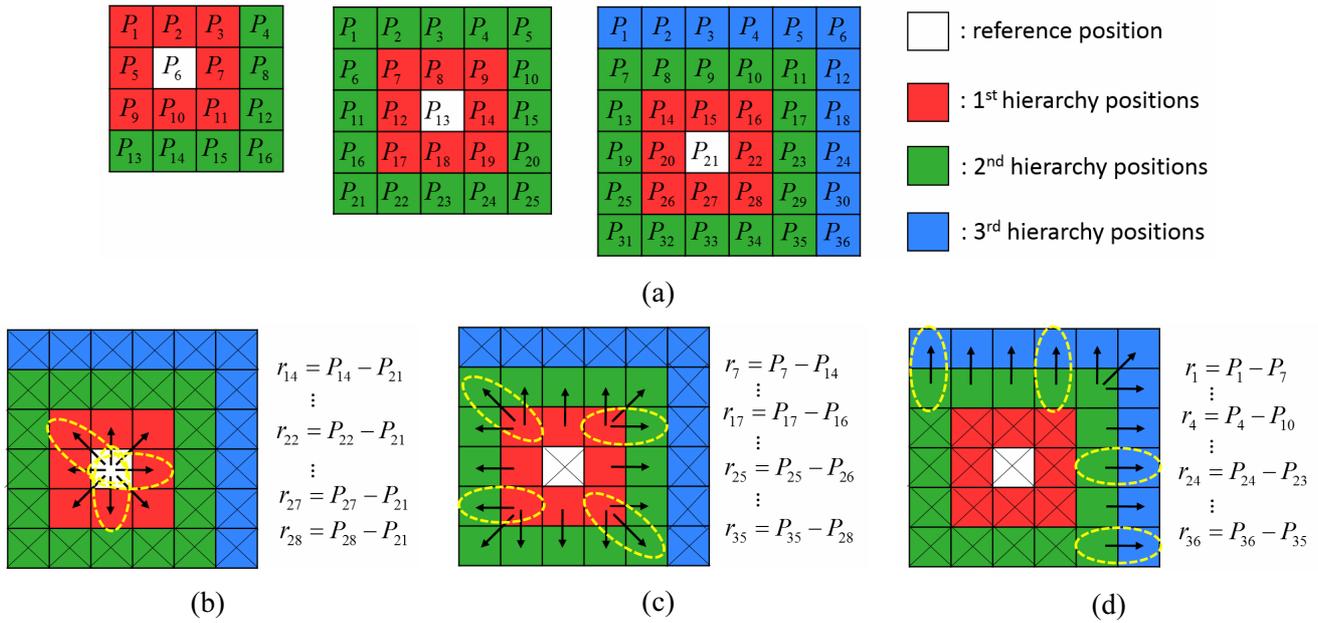
(a)

(b)

(c)

(d)

Figure 3. Illustration of the proposed cascading prediction method

is required, then the method presented in [23] has to search for more number of pairs of the boundary points, but the data-embedding regions cannot be overlapped:

$$[PP_i, ZP_i] \cap [PP_j, ZP_j] = \varnothing, \ i \neq j, \quad \textbf{(5)}$$

where the symbol $\varnothing$ indicates an empty set, and without loss of generality, we assume that $PP_i < ZP_i$ and $PP_j < ZP_j$.

After cascading prediction, the residual histogram is significantly concentrated (an example is presented in Figure 7a in Chapter 4). The advantage of having a concentrated residual histogram is the larger bin value np at the peak point, which equals to having a larger data capacity in the histogram-based data embedding methods. However, for a concentrated residual histogram, it typically looks like a Gaussian function with a quite small variance, which leads to the result that the first data-embedding region $[PP_1, ZP_1]$ is usually significantly wide, and the selection of the second peak point (PP_2) is thus limited.

To address this problem, we proposed a more flexible search rule for finding multiple boundary point pairs as follows. First, all the positions of zero points (i.e. the residual values which have zero bin value) are found, and then, all the nonzero bin values are sorted in a descending order. For the first peak point PP_1 (i.e. the residual value which has the largest bin value), the corresponding zero point ZP_1 is determined by selecting the zero point that is the closest to PP_1. The same procedure is conducted to find the subsequent boundary point pairs, and no zero point is allowed to correspond to multiple peak points. To maintain the image quality, a user-defined parameter α was used to control the largest acceptable distance between a peak point and its corresponding zero point. In other words,

the distance $|PP_i - ZP_i|$ must be smaller than α. Otherwise, the peak point is discarded without carrying data in the data-embedding phase.

3.3 Histogram Modification and Data Embedding

An example of data-embedding with multiple pairs of boundary points is as follows. Assume that an original residual histogram is displayed in Figure 4(a) in which two pairs of boundary points ($PP_1 = 0, ZP_1 = 4$) and ($PP_2 = 1, ZP_2 = 6$) are found. Based on (2), for the first round of histogram modification, the residual values between $PP_1 + 1$ and $ZP_1 - 1$ are shifted to the right by one residual unit. Both PP_2 and ZP_2 are separately modified based on whether they belong to the first data-embedding region as follows:

$$PP_2' = \begin{cases} PP_2 + 1, & \text{if } PP_1 < ZP_1 \text{ and } PP_2 \in [PP_1, ZP_1] \\ PP_2 - 1, & \text{if } PP_1 > ZP_1 \text{ and } PP_2 \in [PP_1, ZP_1] \ ,\textbf{(6)} \\ PP_2, & \text{if } PP_2 \notin [PP_1, ZP_1] \end{cases}$$

and

$$ZP_2' = \begin{cases} ZP_2 + 1, & \text{if } PP_1 < ZP_1 \text{ and } ZP_2 \in [PP_1, ZP_1] \\ ZP_2 - 1, & \text{if } PP_1 > ZP_1 \text{ and } ZP_2 \in [PP_1, ZP_1] \ .\textbf{(7)} \\ ZP_2, & \text{if } ZP_2 \notin [PP_1, ZP_1] \end{cases}$$

To recover the original image, the modified pair (PP_2', ZP_2') is recorded instead of (PP_2, ZP_2). Similarly, for the second round of histogram modification, the residual values between $PP_2' + 1$ and $ZP_2' - 1$ are shifted to the right by one residual unit.

After the histogram modification step by using the two modified pairs, the resulting modified histogram is shown in Figure 4(c). For data embedding, secret bits

(a)

(b)

(c)
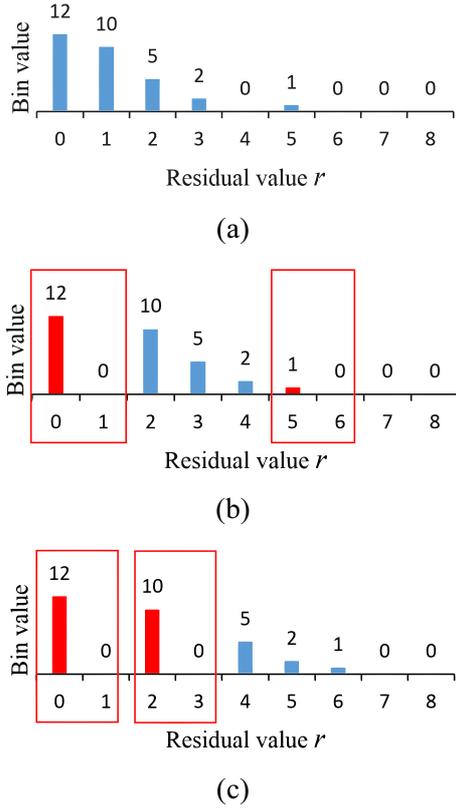
Figure 4. Payload comparison between [23] and the proposed method

are embedded in PP_2' and PP_1 in an ordered manner as follows:

$$r_i' = r_i + s_j, \text{ if } r_i = PP_2' \text{ or } PP_1, \tag{8}$$

where $s_j \in \{0,1\}$ indicates the j-th to-be-embedded secret bit, and r_i' indicates the stego residual value.

At the receiver end, each residual stego-image block is generated by applying the same cascading prediction technique described in Section 3.1. Therefore, the residual histograms of individual image blocks are obtained. Data extraction and recovery are realized when the peak and zero point values are known. The information of (PP_2', ZP_2') is first utilized for examining all the stego residual values r_i', and the hidden secret bits are extracted as follows:

$$\begin{cases} s_j = 1 \text{ and } \breve{r}_i = r_i' - 1, \text{ if } r_i' = PP_2' + 1 \\ s_j = 0 \text{ and } \breve{r}_i = r_i', \text{ if } r_i' = PP_2' \end{cases}. \tag{9}$$

where $\breve{r}_i$ indicates the recovered residual value. Then, the reverse histogram modification is employed within the range of $PP_2' + 1$ and ZP_2'. For data extraction and recovery by using the information of (PP_1, ZP_1), the same procedure is conducted repeatedly.

4 Experimental Results

A large number of experiments were conducted to demonstrate the effectiveness and superiority of the proposed technique. Eight standard 512 × 512 grayscale images, i.e., Airplane (Figure 5(a)), Boat (Figure 5(b)), Girl (Figure 5(c)), Goldhill (Figure 5d), Lenna (Figure 5(e)), Sailboat (Figure 5(f)), Tiffany (Figure 5(g)), Zelda (Figure 5(h)), are shown in Figure 5 were used in the experiments. The simulations were performed on windows 10 PC with an Intel Core i7 3.4 GHz CPU and the 8 GB RAM. The testing programs are implemented by using Bloodshed Dev C++. For notational simplicity, the methods presented in [23], [24], and [25] are referred to as the HS, BPRHS, and CPRHS methods, respectively.

| (a) | (b) | (c) | (d) |

| (e) | (f) | (g) | (h) |

Figure 5. Grayscale test images

In the experiments, in order to measure the visual quality of embedded images, peak signal to noise ratio (PSNR) was utilized, which was a commonly-used objective assessment index for image quality. The greater PSNR value was, the better visual quality of embedded image was. The calculation of PSNR value can be found in Eqs. (10) and (11):

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}, \tag{10}$$

and

$$MSE = \frac{1}{W \times H} \sum_{x=1}^{W} \sum_{y=1}^{H} [I(x, y) - I_e(x, y)]^2, \tag{11}$$

where W and H were the height and the width of the images, respectively; $I(x, y)$ and $I_e(x, y)$ were the pixel values at coordinate (x, y) of the original uncompressed grayscale image I and the embedded image I_e, respectively.

Results of the hiding capacity and the embedded image quality of the histogram shifting (HS) technique are listed in Table 1. Here, *pno* denotes the pairs of the peak and zero points used. According to the results, hiding capacity of the HS technique increases with the increase of the *pno* value. Average hiding capacities of 4486.75 bits and 8683.25 bits are achieved when the *pno* values are set to 1 and 2, respectively. Accordingly, average embedded image qualities of 53.223 dB and 48.266 dB are achieved, respectively (in terms of PSNR). When *pno* is set to 3 in the HS technique, only four out of these eight images can find the required pairs of peaks and zero points for data embedding. However, the gains of the hiding capacity for these four images are 1 bit, 3 bits, 3 bits, 217 bits for these four test images Boat, Girl, Lenna, and Tiffany, respectively.

Table 1. Results of the hiding capacity (unit: bits) and the embedded image quality (unit: dB) of the HS technique

Factors / Images	Hiding Capacity			Embedded Image Quality		
	pno = 1	pno = 2	pno = 3	pno = 1	pno = 2	pno = 3
Airplane	9002	17042	N/A	53.242	48.275	N/A
Boat	5614	10567	10568	53.128	48.219	48.218
Girl	3739	7459	7462	55.223	48.381	48.381
Goldhill	2683	5336	N/A	51.224	48.490	N/A
Lenna	2908	5760	5763	53.850	48.179	48.179
Sailboat	4263	8186	N/A	53.629	48.190	N/A
Tiffany	5120	10153	10370	52.172	48.219	48.217
Zelda	2565	4963	N/A	53.317	48.172	N/A

Table 2 lists the results of the hiding capacity and the embedded image quality of the block-based prediction residual histogram shifting (BPRHS) technique. Average hiding capacities of 23736.375, 44581.875, and 44590 bits were achieved using the BPRHS technique when the *pno* values were set to 1, 2, and 3, respectively. Accordingly, average embedded image qualities of 51.919 dB, 49.288 dB and 49.163 dB are achieved, respectively. Among these test images, Airplane and Sailboat obtains the highest and lowest hiding capacities in the BPRHS technique, respectively. The residual images of these two images generated by the BPRHS technique are depicted in Figure 6 to help the readers understanding the relation between the occurrences of the prediction error and the hiding capacity.

Table 2. Results of the hiding capacity (unit: bits) and the embedded image quality (unit: dB) of the BPRHS technique

Factors / Images	Hiding Capacity			Embedded Image Quality		
	pno = 1	pno = 2	pno = 3	pno = 1	pno = 2	pno = 3
Airplane	36532	63616	63620	52.150	49.713	49.713
Boat	23047	44631	44637	51.864	49.282	49.282
Girl	22442	43746	43767	52.059	49.269	49.268
Goldhill	16463	31903	31909	51.755	49.016	49.016
Lenna	24447	46009	46014	51.924	49.313	49.313
Sailboat	16015	30672	30677	51.728	48.991	48.991
Tiffany	28299	51469	51481	51.990	49.438	49.438
Zelda	22646	44609	44615	51.881	49.283	48.283

(a)   (b)
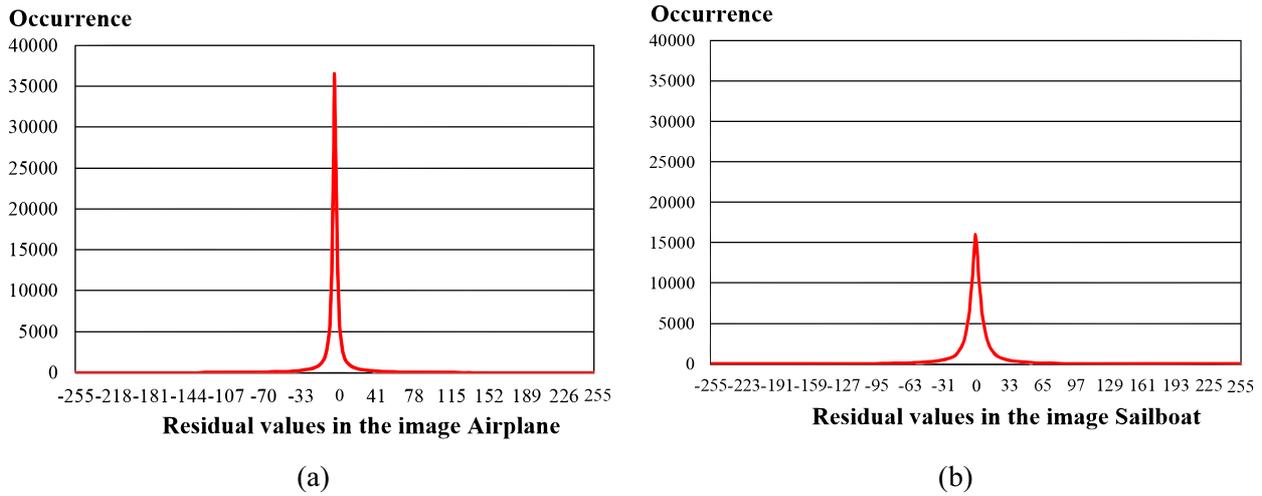
Figure 6. Residual image histograms generated in the BPRHS technique

Table 3 presents the results of the hiding capacity and the embedded image quality of the cascading prediction residual histogram shifting (CPRHS) technique. From the results, average hiding capacities of 27264, 50951.375, and 50957.125 bits were achieved using the CPRHS technique when the *pno* values were set to 1, 2, and 3, respectively. Accordingly, average embedded image qualities of 49.268 dB, 47.698 dB and 47.698 dB are achieved, respectively. The residual images of these two images generated using the CPRHS technique are depicted in Figure 7. Results of the hiding capacity and the embedded image quality of the proposed technique are listed in Figure 8 and Figure 9, respectively. The proposed scheme significantly improves the hiding capacity when the *pno* value is set to 3 compared with the capacities obtained using the BPRHS the *pno* value is set to 3. Results of image quality and capacity of these comparative techniques are depicted in Figure 10. The maximal image qualities of 62.695 dB and 63.284 dB are achieved by the pixel value ordering technique (PVO) [26] and the quadtree-based pixel value

ordering technique (QPVO) [27], respectively. Figure 11 shows the embedded images by using different methods.

5 Conclusion

Data transmission is essential for HCC applications because machine learning requires a considerable amount of training data. In view of the privacy leakage concern on the Internet, ensuring the secure Internet-based communication is an urgent issue. This paper proposed an HS-based data hiding method, which can be applied to image authentication for improving security. The experimental results reveal that the proposed method can maintain a high image visual quality even when a large amount of secret data is embedded in the image. As shown in Table 1, Table 2, and Table 3, the proposed algorithm outperforms the comparative method, especially in terms of data capacity.

Table 3. Results of the hiding capacity (unit: bits) and the embedded image quality (unit: dB) of the CPRHS technique

| Factors / Images	Hiding Capacity			Embedded Image Quality		
	pno = 1	*pno* = 2	*pno* = 3	*pno* = 1	*pno* = 2	*pno* = 3
Airplane	41328	71406	71410	49.540	48.063	48.063
Boat	24938	48116	48121	49.275	47.975	47.974
Girl	26255	51421	51431	49.402	47.373	47.373
Goldhill	19905	38501	38505	49.013	47.315	47.314
Lenna	28785	53776	53783	49.238	47.551	47.550
Sailboat	17137	32950	32952	49.058	47.645	47.645
Tiffany	32074	57419	57428	49.466	48.199	48.199
Zelda	27690	54022	54027	49.148	47.462	47.462
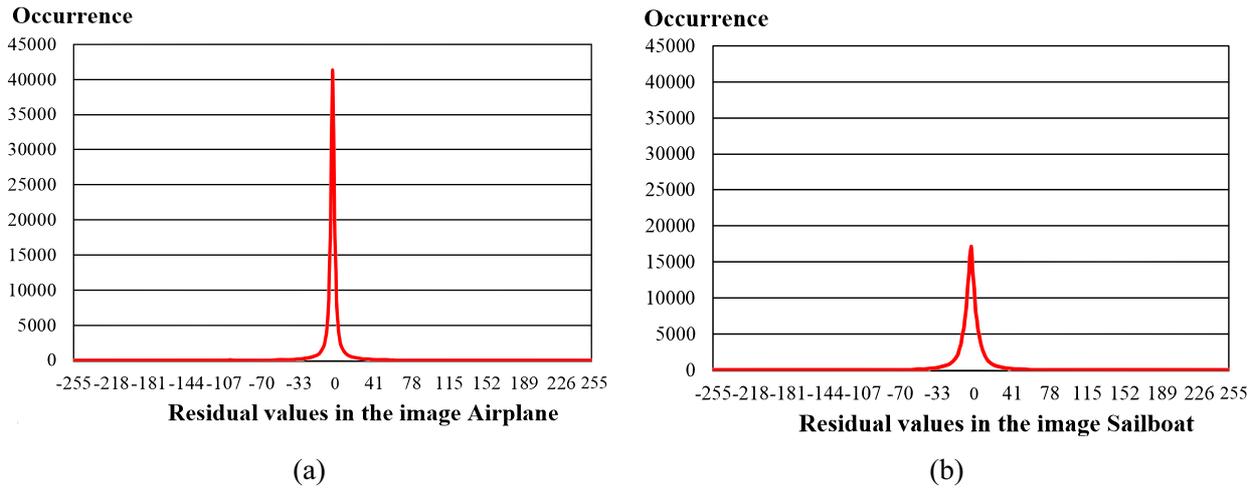
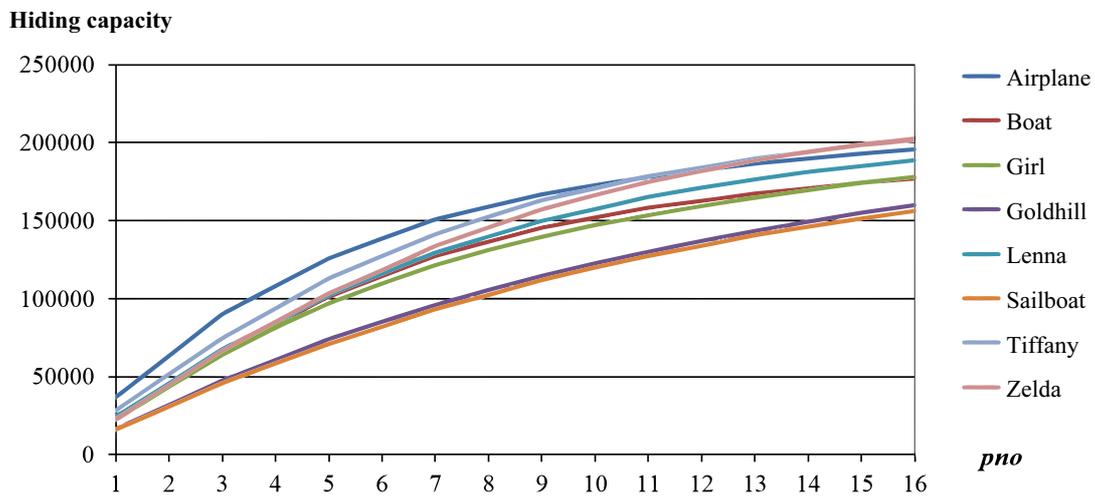**Figure 7.** Residual image histograms generated in the CPRHS technique

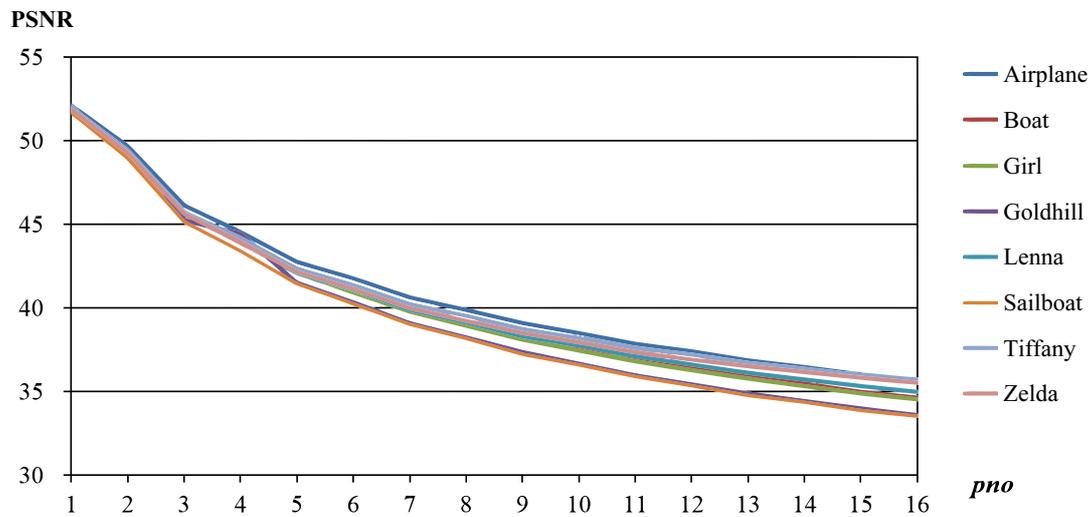**Figure 8.** Results of the hiding capacity of the proposed technique

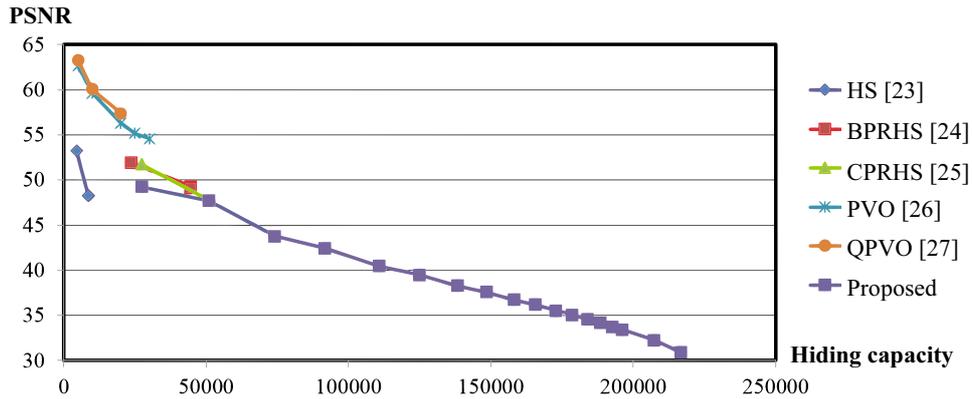**Figure 9.** Results of the image quality of the proposed technique

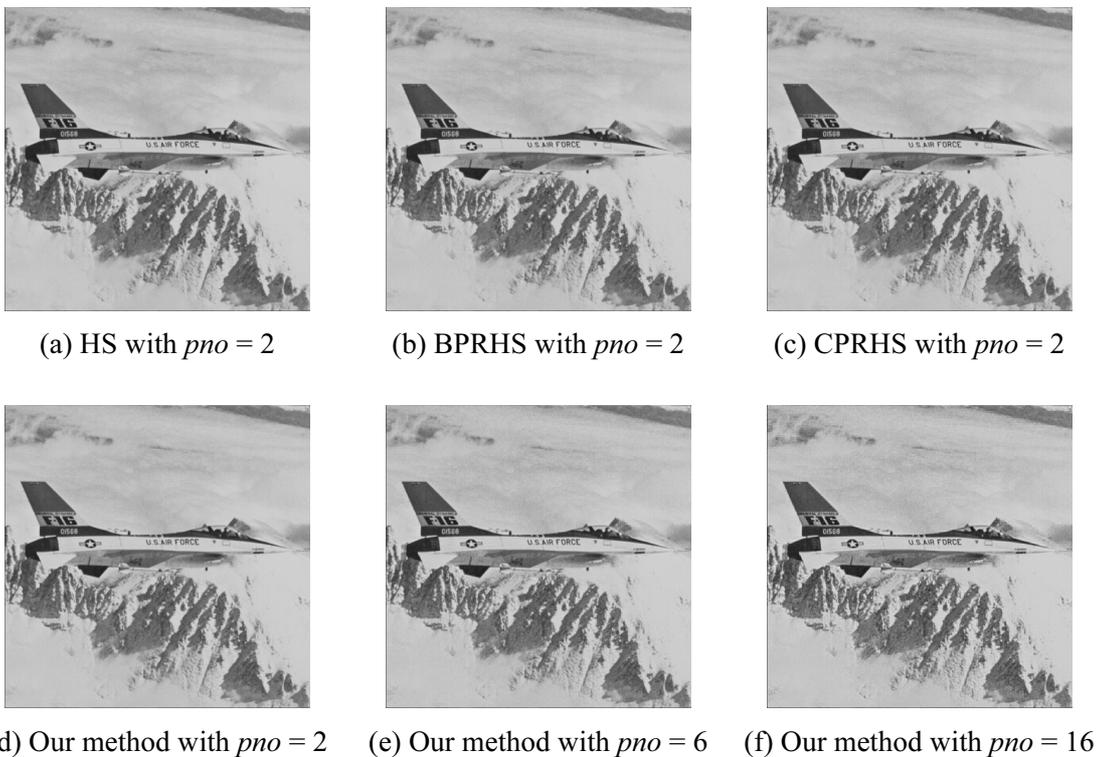**Figure 10.** Performance comparisons among the comparative techniques

(a) HS with *pno* = 2 (b) BPRHS with *pno* = 2 (c) CPRHS with *pno* = 2

(d) Our method with *pno* = 2 (e) Our method with *pno* = 6 (f) Our method with *pno* = 16

Figure 11. Embedded images of Airplane by using different techniques

Acknowledgements

References

[1] C. Yin, S. Ding, J. Wang, Mobile Marketing Recommendation Method Based on User Location Feedback, *Human-centric Computing and Information Sciences*, Vol. 9, pp. 1-17, May, 2019.

[2] B. Vos, F. Berendsen, M. Viergever, H. Sokooti, M. Staring, I. Isgum, A Deep Learning Framework for Unsupervised Affine and Deformable Image Registration, *Medical Image Analysis*, Vol. 52, pp. 128-143, February, 2019.

[3] J. Lee, J. Jung, P. Park, S. Chung, H. Cha, Design of a Human-centric De-identification Framework for Utilizing Various Clinical Research Data, *Human-centric Computing and Information Sciences*, Vol. 8, pp. 1-12, June, 2018.

[4] F. Xiao, M. Lu, Y. Zhao, S. Menasria, D. Meng, S. Xie, J. Li, C. Li, An Information-aware Visualization for Privacy-preserving Accelerometer Data Sharing, *Human-centric Computing and Information Sciences*, Vol. 8, pp. 1-28, May, 2018.

[5] H. Kim, Y. Jeong, Secure Authentication-management Human-centric Scheme for Trusting Personal Resource Information on Mobile Cloud Computing with Blockchain, *Human-centric Computing and Information Sciences*, Vol. 8, pp. 1-13, May, 2018.

[6] V. Mohammadi, A. Rahmani, A. Darwesh, A. Sahafi, Trust-

based Recommendation Systems in Internet of Things: A Systematic Literature Review, *Human-centric Computing and Information Sciences*, Vol. 9, pp. 1-61, June, 2019.

[7] N. Wu, M. Hwang, A Novel Lsb Data Hiding Scheme with the Lowest Distortion, *The Imaging Science Journal*, Vol. 65, No. 6, pp. 371-378, July, 2017.

[8] S. Shen, L. Huang, A Data Hiding Scheme Using Pixel Value Differencing and Improving Exploiting Modification Directions, *Computers & Security*, Vol. 48, pp. 131-141, February, 2015.

[9] Y. Liu, C. Yang, Q. Sun, Enhance Embedding Capacity of Generalized Exploiting Modification Directions in Data Hiding, *IEEE Access*, Vol. 6, pp. 5374-5378, December, 2017.

[10] X. Zhang, Z. Sun, Z. Tang, C. Yu, X. Wang, High Capacity Data Hiding Based on Interpolated Image, *Multimedia Tools and Applications*, Vol. 76, No. 7, pp. 9195-9218, April, 2017.

[11] C. Yang, S. Hsu, C. Kim, Improving Stego Image Quality in Image Interpolation Based Data Hiding, *Computer Standards & Interfaces*, Vol. 50, pp. 209-215, February, 2017.

[12] X. Cao, L. Du, X. Wei, D. Meng, X. Guo, High Capacity Reversible Data Hiding in Encrypted Images by Patch-level Sparse Representation, *IEEE Transactions on Cybernetics*, Vol. 46, No. 5, pp. 1132-1143, May, 2016.

[13] X. Liao, C. Shu, Reversible Data Hiding in Encrypted Images Based on Absolute Mean Difference of Multiple Neighboring Pixels, *Journal of Visual Communication and Image Representation*, Vol. 28, pp. 21-27, April, 2015.

[14] F. Huang, X. Qu, H. Kim, J. Huang, Reversible Data Hiding in Jpeg Images, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 26, No. 9, pp. 1610-1621, September, 2016.

[15] T. Lu, C. Tseng, J. Wu, Dual Imaging-based Reversible Hiding Technique Using Lsb Matching, *Signal Processing*, Vol. 108, pp. 77-89, March, 2015.

[16] X. Liao, K. Li, J. Yin, Separable Data Hiding in Encrypted Image Based on Compressive Sensing and Discrete Fourier Transform, *Multimedia Tools and Applications*, Vol. 76, No. 20, pp. 20739-20753, October, 2016.

[17] I. Chang, Y. Hu, W. Chen, C. Lo, High Capacity Reversible Data Hiding Scheme Based on Residual Histogram Shifting for Block Truncation Coding, *Signal Processing*, Vol. 108, pp. 376-388, March, 2015.

[18] X. Li, W. Zhang, X. Gui, B. Yang, Efficient Reversible Data Hiding Based on Multiple Histograms Modification, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 9, pp. 2016-2027, September, 2015.

[19] H. Chen, J. Ni, W. Hong, T. Chen, Reversible Data Hiding with Contrast Enhancement Using Adaptive Histogram Shifting and Pixel Value Ordering, *Signal Processing: Image Communication*, Vol. 46, pp. 1-16, August, 2016.

[20] M. Li, Y. Li, Histogram Shifting in Encrypted Images with Public Key Cryptosystem for Reversible Data Hiding, *Signal Processing*, Vol. 130, pp. 190-196, January, 2017.

[21] Y. Li, S. Yao, K. Yang, Y. Tan, Q. Zhang, A High-imperceptibility and Histogram-shifting Data Hiding Scheme for Jpeg Images, *IEEE Access*, Vol. 7, pp. 73573-73582, May, 2019.

[22] S. Li, K. Gu, Smart Fault-detection Machine for Ball-bearing System with Chaotic Mapping Strategy, *Sensors*, Vol. 19, No. 9, pp. 1-16, May, 2019.

[23] Z. Ni, Y. Shi, N. Ansari, W. Su, Reversible Data Hiding, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 3, pp. 354-362, March, 2006.

[24] P. Tsai, Y. Hu, H. Yeh, Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting, *Signal Processing*, Vol. 89, No. 6, pp. 1129-1143, June, 2009.

[25] Y. Hu, P. Tsai, J. Yeh, W. Chen, Residual Histogram Shifting Technique Based on Cascading Prediction for Reversible Data Hiding, *International Conference on Future Information Technology*, Hanoi, Vietnam, 2015, pp. 105-110.

[26] X. Li, J. Li, B. Li, B. Yang, High-fidelity Reversible Data Hiding Scheme Based on Pixel-value-Ordering and Prediction-error Expansion, *Signal Processing*, Vol. 93, No. 1, pp. 198-205, January, 2013.

[27] F. Di, M. Zhang, X. Liao, J. Liu, High-fidelity Reversible Data Hiding by Quadtree-based Pixel Value Ordering, *Multimedia Tools and Applications*, Vol. 78, No. 6, pp. 7125-7141, March, 2019.

Biographies

Yung-Yao Chen received his Ph.D. degree in Electrical Engineering from Purdue University, USA in 2013. He is currently an Associate Professor in the Dept. Electronic and Computer Engineering, National Taiwan U. Science and Technology, Taipei, Taiwan. His research interests include image and signal processing, halftoning, computer vision, and human-computer interaction.

Chih-Hsien Hsia received the Ph.D. degree in Electrical Engineering from Tamkang University, New Taipei, Taiwan, in 2010. He currently is an Associate Professor with the Department of Computer Science and Information Engineering, National Ilan University, Taiwan. His research interests include DSP IC Design, Multimedia Signal Processing, and Information Education.

Hsiang-Yun Kao received the B.S. degree in Electronic Engineering from Chang Gung University, Taoyuan, Taiwan, in 2017. He is currently pursuing the M.S. degree with the Graduate Institute of Automation Technology, National Taipei University of Technology, Taipei, Taiwan. His current research interests include digital image processing and information security.

You-An Wang received the B.S. degree in Electrical Engineering from National University of Tainan, Tainan, Taiwan. He is currently pursuing the M.S. degree with the Graduate Institute of Automation Technology, National Taipei University of Technology, Taipei, Taiwan. His current research interests include digital image processing and information security.

Yu-Chen Hu received his PhD. degree in computer science and information engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan in 1999. Currently, Dr. Hu is a professor in the Department of Computer Science and Information Management, Providence University, Taiwan. His research interests include digital forensics, information hiding, image and signal processing, data compression, information security, and data engineering.