EURASIP Journal on Image and Video Processing

RESEARCH Open Access

High-capacity reversible image steganography based on pixel value ordering

Hsing-Han Liu* and Chuan-Min Lee

Abstract

In this study, an improved reversible image steganography method based on pixel value ordering (PVO) is proposed to improve the steganographic capacity. Before the steganography process, three continuous and neighboring pixels are regarded as one group for sequencing, where the maximum and minimum values are adopted for difference value calculation and the number of difference values is recorded. The pixels with more steganographic difference values in rows or columns are determined, after which the steganography and ciphertext retrieval steps are performed in the rows or columns of the digital image. The experiment results prove that the method replaces the block structure in frame selection by groups of continuously read pixels, i.e., every three pixels form a pixel group where two bits of confidential information can be hidden, thus improving the steganographic capacity effectively. Comparisons with other PVO hiding schemes confirm the superiority of the proposed scheme, which has a higher capacity and maintains an acceptable peak signal-to-noise ratio (PSNR).

Keywords: Reversible information hiding, Pixel-value-ordering, Steganography capacity

1 Introduction

The development of information technology and the widespread use of smartphones have contributed to the ever-growing frequency of interpersonal communication in modern society. However, information can be leaked through illegal or intentional actions of personnel during information transmission, resulting in severe losses. From the perspective of historical development, information hiding is an effective way to transmit confidential information. Consequently, advanced information hiding techniques are extensively applied to various modern digital images and other media. Information hiding techniques hide confidential information and display meaningful content in such a manner that suspicion is not easily aroused. Information hiding technologies can be classified as shown in Fig. 1 [1].

Information hiding techniques are extensively utilized in various fields, such as military and commercial communications, primarily for the transmission of digital image content. Because it is difficult for the naked eye to spot the minute differences in the digital image content, human beings are usually unable to notice the hidden confidential information.

With the rapid development of information hiding technologies, methods for steganographic capacity improvement and digital image quality evaluation have emerged as a major research topic. Steganography techniques include the least-significant bit (LSB) [2], pixel-value differencing (PVD) [3], and subsequently proposed substitution and combination methods of PVD and LSB [4]. The steganography method based on LSB and PVD is classified as a lossy data hiding approach. Further, the histogram shifting method [5] is a lossless data hiding approach that causes the least distortion to images and results in higher image quality after steganography; hence, it has attracted considerable attention from researchers [6–8]. Zhang proposed a novel reversible data hiding scheme for encrypted images. In the proposed scheme, after encrypting the entire data of an uncompressed image by a stream cipher, the additional data is embedded into the image by modifying a small proportion of the encrypted data [9]. Qin et al. proposed a novel joint data hiding and compression scheme for digital images that uses side match vector quantization

* Correspondence: liu.hansh@gmail.com
National Defense University, No. 70, Sec. 2, Zhongyang N. Rd., Beitou District, Taipei City 11258, Taiwan, Republic of China

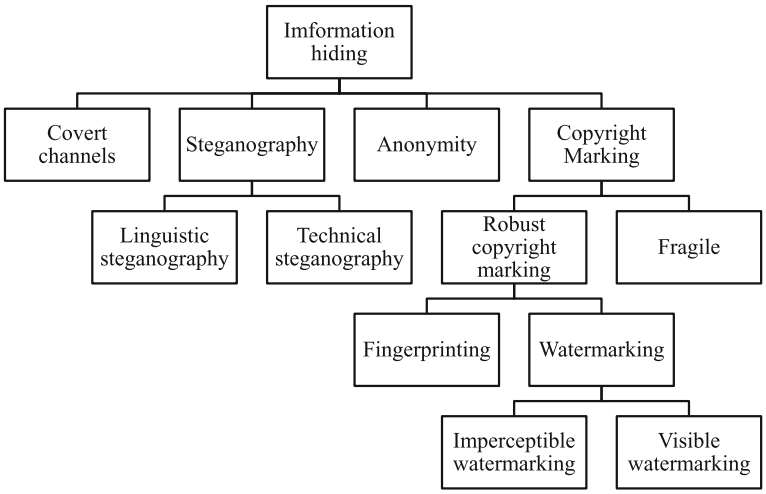


Fig. 1 Classification of information hiding technologies. The four types of information hiding technologies are covert channels, steganography, anonymity, and copyright marking

(SMVQ) and image inpainting. The data hiding and image compression functions are seamlessly integrated into one single module [10]. Huang et al. proposed multi-level reversible data hiding with a pyramidal structure. Considering the inherent characteristics of the original content and their spatial relationships, a pyramidal structure is employed in which more secret information is hidden with similar quality in the output image [11].

To further improve the steganographic capacity, prediction error histogram shifting (PEHS) steganography, which combines the prediction error (PE) and histogram shifting (HS), has emerged as a well-known technique among currently used lossless data hiding methods [12–14]. In the lossless data hiding approach based on pixel value ordering (PVO) [15], a digital image is sliced into several blocks that are arranged according to the pixel value in each block. Two differences are obtained through subtraction of the largest pixel value and the second largest pixel value as well as subtraction of the smallest pixel value and the second smallest pixel value. However, only the largest pixel value, the smallest pixel value, and their difference within blocks are used for steganography to achieve such excellent image quality. Therefore, there remains a room for improvement of the steganographic capacity. Toward this end, researchers have proposed improved steganography based on PVO [16–19]. The various steganographic methods are compared in Table 1. LSB, PVD, and PVD+LSB are lossy data hiding approaches (no additional information is embedded)—after the extraction of the ciphertext, the original cover image cannot be restored. HS, PEHS, and PVO are lossless data hiding approaches (additional information is embedded)—after the extraction of the ciphertext, the original cover image can be restored. The lossy data hiding approach is suitable for cases where a large amount of ciphertext needs to be transmitted, and the cover image is not required to be restored. The lossless data hiding approach is suitable for transmitting the ciphertext and then recovering the carrier image. The embedded capacity (EC) of various steganographic methods was generated by the experiment. The values in parentheses represent the ratio of embedded capacity divided by the image size (maximum possible embedding capacity). The experimental image used in this study is 512 × 512 grayscale image, and the image size is 262,144.

Steganographic methods employ various techniques to provide security. LSB hides the encrypted message by replacing the least significant bits of the pixels of the cover image. However, sequentially flipping the LSBs can result in the pair of value (PoV) problem [20], which has been

Table 1 Comparison of the various steganographic methods

	LSB [2]	PVD [3]	PVD+LSB [4]	HS [5]	PEHS [11]	PVO [13]
Data hiding approach	Lossy			Lossless		
Embedded capacity (the ratio of EC divided by the image size)	262,144 (1)	409,807 (1.56)	818,538 (3.12)	2716 (0.01)	77,479 (0.3)	31,523 (0.12)
PSNR	51.14	41.16	38.68	51.06	41.05	52.63
Extra information embedding	No	No	No	Yes	Yes	Yes
Security analysis	RS, x^2	Step effect in the PVD histogram		Special feature of the histogram		

explored by many steganalysis methods, such as x^2 [20] and RS [21]. For steganalysis of PVD-based embedding, Zhang and Wang [22] analyzed the histogram of stego images embedded by PVD and proposed a steganalysis technique that attacks the original PVD successfully by exploiting the step effect in the PVD histogram. For steganalysis of HS-based embedding, based on a special feature when all the pixels of the peak point are used to embed the secret message, Kuo et al. [23] proposed specific steganalysis methods to detect Ni's method. Liu and Liu [24] proposed a steganalysis method based on the payload invariant features to detect the histogram shift-based steganography in Ni's method.

On the basis of the background and motivation presented above, in this work, an improvement was achieved mainly by focusing on PVO. The contributions of this work were listed as follows:

(1) The proposed PVO scheme has a higher capacity than the other PVO methods while maintaining an acceptable PSNR, demonstrating the superiority of the proposed hiding scheme.
(2) To verify the suitability of the proposed PVO scheme for various image types, 9,074,512 × 512 grayscale images were selected from the BOWS-2 image databases as raw images. Experimental results proved that the proposed PVO scheme is applicable to different types of images.

The remainder of this paper is organized as follows: Section 2 summarizes the literature related to this research. Section 3 explains the proposed method. Section 4 discusses the related experiments conducted and the proposed hiding scheme. Finally, Section 5 presents our conclusions.

2 Literature review

2.1 Original PVO

PVO is a reversible digital image steganography method proposed by Li et al. [15]. In this method, the digital image is sliced into several blocks and ordering is performed according to the pixel values in each block. The difference between the largest pixel value and the second largest pixel value and the difference between the smallest pixel value and the second smallest value are obtained for steganography with 1 or − 1 as the peak value point b. The steganography steps are shown in Fig. 2.

The ciphertext retrieval steps are shown in Fig. 3.

2.2 Improved PVO

On the basis of the PVO proposed by Li et al. [15], Peng et al. [16] proposed the improved PVO (IPVO) for reversible digital image steganography. In contrast to PVO, where the differences are obtained from the subtraction of the largest and the second largest pixel values and the smallest and the second smallest pixel values inside the calculation blocks, the subtraction order is determined according to the reading order. In other words, the obtained differences can be positive or negative, and more differences are obtained compared to PVO. Further, "0" and "1" are applied as the peak points of differences for steganography. Thus, compared to PVO, IPVO achieves a better peak signal-to-noise ratio (PSNR) value under higher steganographic capacity [25].

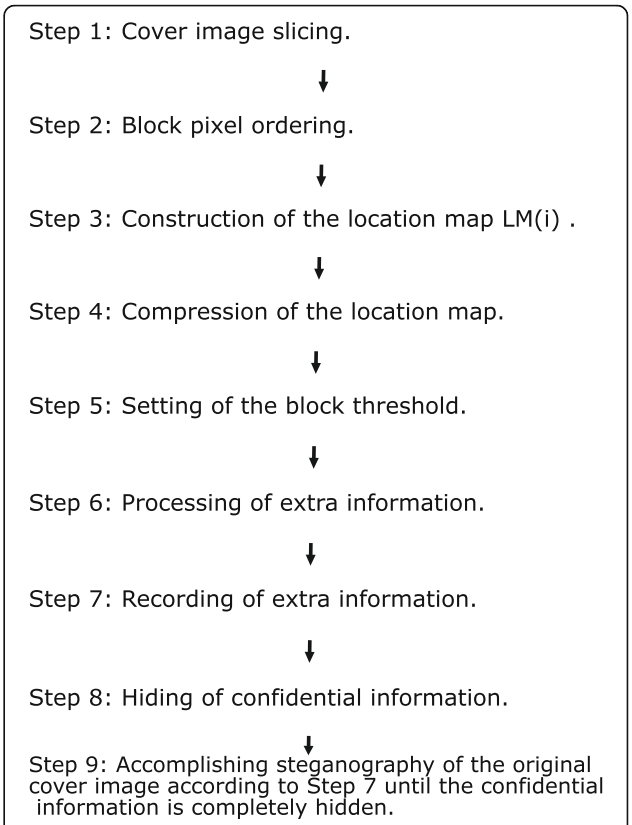


Fig. 2 Steps in the PVO steganography method. (1) Cover image slicing. (2) Block pixel ordering. (3) Construction of the location map $LM_{(i)}$. (4) Compression of the location map. (5) Setting of the block threshold. (6) Processing of extra information. (7) Recording of extra information. (8) Hiding of confidential information. (9) Accomplishing steganography of the original cover image according to step 7 until the confidential information is completely hidden

2.3 PVO multi-pixel modification

On the basis of the PVO proposed by Li et al. [15] and the IPVO proposed by Peng et al. [16], Chen et al. [19] proposed a digital image steganography method based on pixel order exchange and multi-pixel modification, called PVO multi-pixel modification (PVOMM). Compared to PVO and IPVO, after accomplishing the ordering of block slicing, the order in PVOMM is the largest, second largest, second smallest, and smallest pixel values. The second largest pixel value acts as the benchmark for this block, and subtraction of that value from

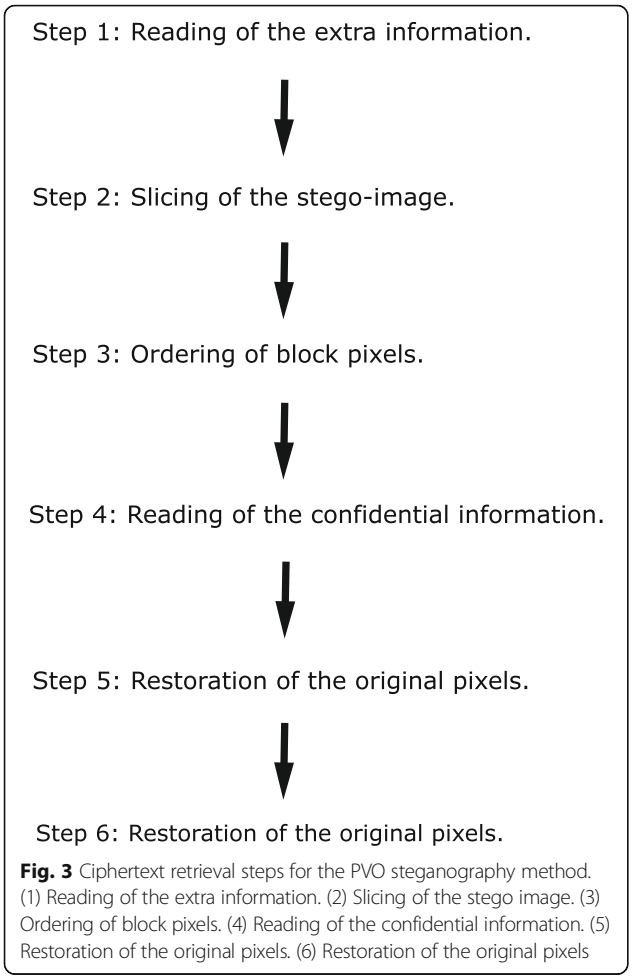


Fig. 3 Ciphertext retrieval steps for the PVO steganography method. (1) Reading of the extra information. (2) Slicing of the stego image. (3) Ordering of block pixels. (4) Reading of the confidential information. (5) Restoration of the original pixels. (6) Restoration of the original pixels

the largest, second largest, and smallest pixel values is conducted. When four pixel values constitute a group, three differences can be obtained. However, the scenario that the largest and the second largest pixel values simultaneously meet the steganography conditions must be excluded. Thus, it is feasible to restore the original cover image without influencing the original pixel ordering positions. Table 2 compares and contrasts the three PVO-based methods [25].

3 Proposed methods

3.1 Pixel group selection methods

The aim of the study was to improve the steganographic capacity by modifying the original PVO method. In addition to adjusting the block selection size, the middle pixel value in the ordering block is used. The middle pixel value is subtracted from the maximum and minimum pixel values, which yields more differences compared to PVO.

The PVO methods discussed above employ the block as the core component; hence, steganography is conducted by using different steganographic algorithms or by selecting expressions after adjusting the block size, depending on which the steganographic capacity or image quality is improved. However, such improvement is limited within the block framework. Therefore, in this study, pixel-by-pixel processing, which has not been used previously, is used to read the pixel values in order in columns or rows. Furthermore, calculations are performed by regarding every three pixel values as one group.

Table 2 Similarities and differences points among the three PVO-based methods [25]

	PVO	IPVO	PVOMM
Similarities			
Pixel values need to be sorted in the processing unit.			
Secret information embedded by expanding the prediction error.			
Extra information has to be considered (handle the overflow/underflow problem).			
High image quality preserved after embedding secret information.			
"Fixed block" method used.			
Differences			
Peak points	"1" or "− 1"	"0" and "1" (or "− 1")	"1" or "− 1"

In this study, to maximize the steganographic capacity of a digital image, before image steganography, reading in order in rows and columns (see Fig. 4) is performed, respectively. After obtaining the available steganographic capacity of the digital image for comparison, the reading method of the digital image is recorded. In the same digital image, the reading position of the first and the last pixel values remains the same in row or column reading; hence, the reading method will be recorded in the last pixel value in the entire digital image by the LSB as the first restored information after determining the reading method.

3.2 Steganography and ciphertext retrieval methods

The following are the steganography and ciphertext retrieval methods:

Step 1: The LSB of the final pixel value in the digital image will be used to indicate whether the digital image is read in row or column order. This leads to the advantage of lossless restoration of the stego image. Thus, the final pixel value of the cover image is transformed into the binary format, and it is recorded as 0 or 1.

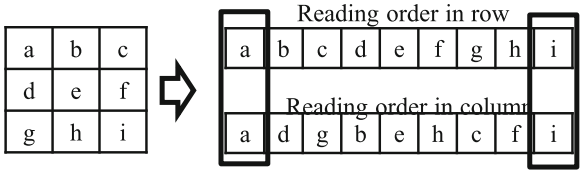


Fig. 4 Reading order example of the image. In this study, to maximize the steganographic capacity of a digital image, before image steganography, reading in order in rows and columns is performed, respectively

Step 2: The cover image is read in row and column order, and the differences are calculated. If the difference is maximum while reading in rows, it is recorded as 1. If the difference is maximum while reading in columns, it is recorded as 0. This value is stored in the final pixel value of the digital image by using the LSB.

Step 3: Block pixel ordering. The sliced area pixel values p_1, p_2, and p_3 are rearranged in order, through which the sequences $p_{\sigma(1)}$, $p_{\sigma(2)}$, and $p_{\sigma(3)}$ are obtained, where $p_{\sigma(1)} \geq p_{\sigma(2)} \geq p_{\sigma(3)}$.

Step 4: Construction of the location map $LM_{(i)}$. In this method, the largest or the smallest pixel value is adjusted; hence, the overflow problem can occur if the largest or the smallest pixel value is 255 or 0, respectively. Therefore, it is necessary to determine whether the block is an overflow block before the steganography steps; the relevant equation is given below.

$$\begin{cases} p_{\sigma(1)} - p_{\sigma(2)} \geq 1 \text{ and } p_{\sigma(1)} = 255 \\ p_{\sigma(3)} - p_{\sigma(2)} \leq 1 \text{ and } p_{\sigma(3)} = 0 \end{cases} \quad (1)$$

If the block satisfies the conditions of Eq. 1, the block is an overflow block that is marked as $LM_{(i)} = 1$. If there is no overflow problem, $LM_{(i)} = 0$.

Step 5: Compression of the location map. The location map $LM_{(i)}$ is a series of binary information of length k that is compressed into l_{clm} through arithmetic coding. There are fewer blocks with overflow problems in the original cover images; hence, there are fewer points where $LM_{(i)} = 1$. Through arithmetic coding, lossless compression can be used to compress the location map in order to reduce the production of extra information.

Step 6: Processing of extra information. The information used during the steganography process of the original cover image is listed below:

- If the evidence is read in row or column order, 0 or 1 is recorded by the final pixel value, respectively.
- The final index value of the extra information (k_{end}): $\log_2 N$ bits, $N = m \times n$.
- The length of the compressed location map (l_{clm}): $\log_2 N$ bits.
- The compressed location map l_{clm}.
- All the extra information above uses $1 + 2 \log_2 N + l_{clm}$ bits in total.

Step 7: Recording of extra information. The aforementioned extra information is hidden in the original cover image by using the LSB; the replaced bit is represented by S_{LSB} and hidden in each block along with the confidential information.

Step 8: Hiding of confidential information. In the block $LM_{(i)} = 0$ without overflow problems, the largest and the smallest pixel values among the pixel values after ordering according to step 3 are selected to be subtracted along with the second largest pixel value, through which two differences, $d_{\max}$ and $d_{\min}$, are obtained using the following equations.

$$\begin{cases} d_{\max} = p_{\sigma(1)} - p_{\sigma(2)} \\ d_{\min} = p_{\sigma(3)} - p_{\sigma(2)} \end{cases} \quad (2)$$

Next, the differences 1 and − 1 are used for hiding the confidential information b. In view of the differences larger than 1 or smaller than − 1, 1 is added to or subtracted from the largest or the smallest pixel value for difference shifting. When the difference is 0, there is no operation. The new pixel values $d'_{\max}$ and $d'_{\min}$ are obtained after accomplishing difference shifting according to the conditions above. The steganography equations are given below.

$$d'_{\max} = \begin{cases} d_{\max} & , \text{if } d_{\max} = 0 \\ d_{\max} + b, & \text{if } d_{\max} = 1 \\ d_{\max} + 1, & \text{if } d_{\max} > 1 \end{cases} \quad (3)$$

$$d'_{\min} = \begin{cases} d_{\min} & , \text{if } d_{\min} = 0 \\ d_{\min} - b, & \text{if } d_{\min} = -1 \\ d_{\min} - 1, & \text{if } d_{\min} < -1 \end{cases} \quad (4)$$

where $b \in \{0, 1\}$ is a data bit to be embedded. Then, the new largest and smallest pixel values are calculated according to the original largest and smallest pixel values using the following equations:

$$\begin{cases} d'_{\max} = p'_{\sigma(1)} - p_{\sigma(2)} \Rightarrow p'_{\sigma(1)} = d'_{\max} + p_{\sigma(2)} \\ d'_{\min} = p'_{\sigma(3)} - p_{\sigma(2)} \Rightarrow p'_{\sigma(3)} = d'_{\min} + p_{\sigma(2)} \end{cases} \quad (5)$$

Finally, the stego image is obtained after replacing the original pixel values. The step of hiding confidential information is completed.

Step 9: Steganography of the original cover image is carried out according to step 8 until the confidential information is hidden completely. The stego image X' after steganography is obtained.

A flowchart of the steganography method proposed in this study is shown in Fig. 5.

The ciphertext retrieval steps of the steganography method proposed in this study are as follows:

Step 1: Transform the final pixel value of the stego image into the binary format; read the final value as 0 or 1.

Step 2: Read the values extracted from step 1 in rows or columns targeting the stego image.

Step 3: Read the extra information, i.e., $1 + 2 \log_2 N + l_{clm}$ bits.

Step 4: Read the pixel values in order and list them with every three pixel values as one group. Obtain the sequence of pixel values p_1, p_2, and p_3; list them and obtain the sequence $p_{\sigma(1)}$, $p_{\sigma(2)}$, and $p_{\sigma(3)}$, where $p_{\sigma(1)} \geq p_{\sigma(2)} \geq p_{\sigma(3)}$.

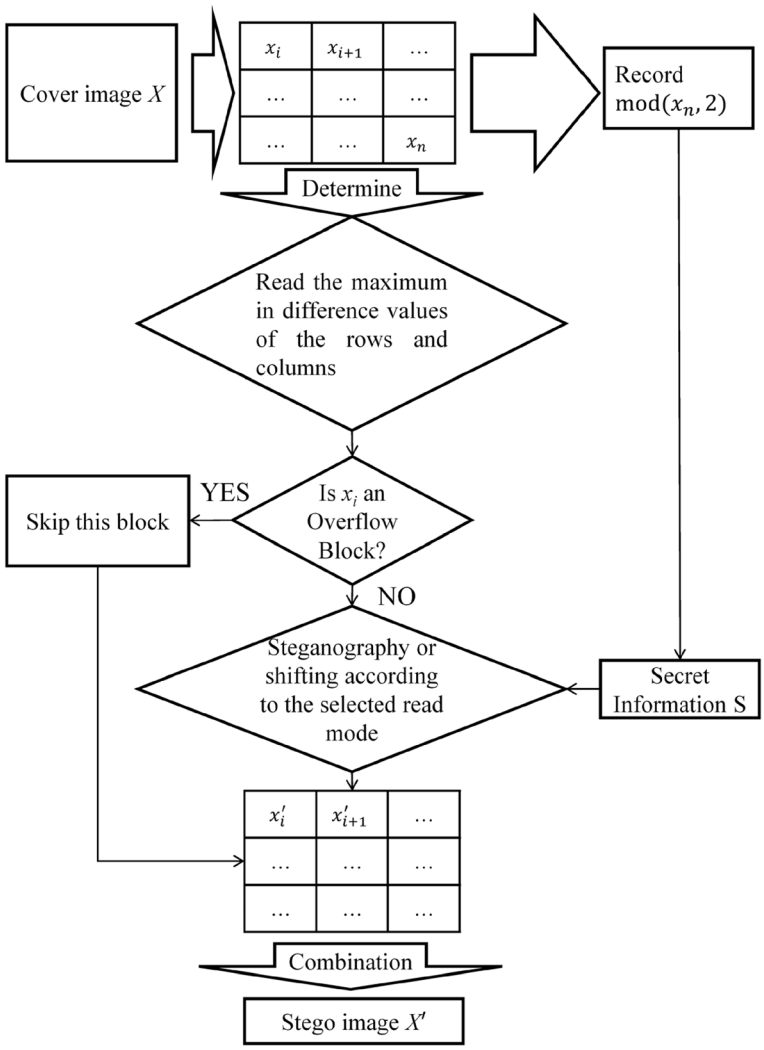


Fig. 5 Flowchart of the steganography method proposed in this study. The steganography steps proposed in this study are described as follows. (1) The LSB of the final pixel value in the digital image will be used to indicate whether the digital image is read in row or column order. (2) The cover image is read in row and column order, and the differences are calculated. (3) Block pixel ordering. (4) Construction of the location map $LM_{(i)}$. (5) Compression of the location map. (6) Processing of extra information. (7) Recording of extra information. (8) Hiding of confidential information. (9) Steganography of the original cover image is carried out according to step 8 until the confidential information is hidden completely

Step 5: According to the extra information, determine whether the sequence is an overflow block.
Step 6: If there is no overflow problem, the selection region is restored for ciphertext retrieval and pixel value restoration using the equations given below.

$$b = \begin{cases} b = 0, \text{if} \quad d'_{\max} = 1 \\ b = 1, \text{if} \quad d'_{\max} = 2 \\ b = 0, \text{if} \quad d'_{\min} = -1 \\ b = 1, \text{if} \quad d'_{\min} = -2 \end{cases} \tag{6}$$

where $b \in \{0, 1\}$ is a data bit to be extracted.

$$d_{\max} = \begin{cases} d'_{\max} \quad , \text{if} \quad d'_{\max} = 1 \\ d'_{\max} - 1, \text{if} \quad d'_{\max} \geq 2 \end{cases} \tag{7}$$

$$d_{\min} = \begin{cases} d'_{\min} \quad , \text{if} \quad d'_{\min} = -1 \\ d'_{\min} + 1, \text{if} \quad d'_{\min} \leq -2 \end{cases} \tag{8}$$

$$\begin{cases} d_{\max} = p_{\sigma(1)} - p_{\sigma(2)} \Rightarrow p_{\sigma(1)} = d_{\max} + p_{\sigma(2)} \\ d_{\min} = p_{\sigma(3)} - p_{\sigma(2)} \Rightarrow p_{\sigma(3)} = d_{\min} + p_{\sigma(2)} \end{cases} \tag{9}$$

Step 7: Restore the cover image. Ciphertext retrieval and restoration are accomplished successively according to step 4, step 5, and step 6, through which the original cover image X is obtained.

A flowchart of the ciphertext retrieval process in the steganography method proposed in this study is shown in Fig. 6.

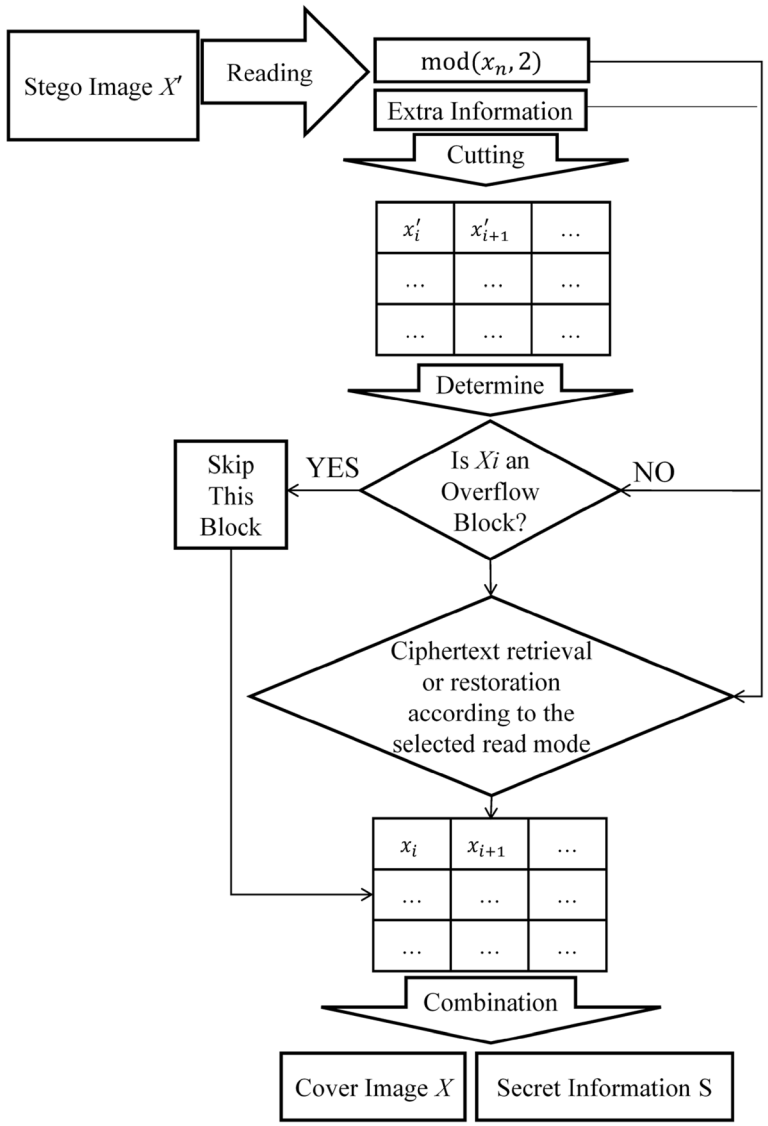


Fig. 6 Flowchart of ciphertext retrieval in the steganography method proposed in this study. The ciphertext retrieval steps of the steganography method proposed in this study are described in Fig. 4

4 Experimental results and discussion

Improvement in the steganographic capacity of digital image steganography based on PVO was the main focus of the preliminary construction period of this study. Thus, in this study, an adjustment was made for calculation based on consideration of every three pixel values as one group, after which the steganographic capacity of the digital image was maximized through scanning in rows and columns.

The proposed PVO hiding scheme was then experimentally evaluated to assess whether its algorithm can increase the hiding capacity while maintaining the acceptable image quality. We also compared the results of the proposed PVO scheme to those of conventional PVO hiding methods to verify its efficiency. The experimental environment, procedures, and results are presented separately below.

4.1 Experimental environment and procedure

The software and hardware experimental environments used in the experiments were as follows:

(1) Hardware environment: Intel(R) Core(TM) i5-4570 CPU at 3.20 GHz 16 GB RAM notebook.
(2) Simulation program: MATLAB was used to implement both the proposed and conventional PVO hiding schemes.
(3) Secret message: the random number generator in MATLAB was used to simulate the ciphertext in the experiments.

(4) Test images: eight 512 × 512 grayscale test images that are widely used in the information hiding field were employed in this study (as shown in Fig. 7), including images with complex and smooth textures, images with portrait and landscape orientations, and images of goods and transportation.
(5) Image databases: to verify the suitability of the hiding scheme for various image types, 9074 512 × 512 grayscale images were selected from the BOWS-2 [26] image databases as raw images (some example images are shown in Fig. 8).

4.2 Steganographic image quality analysis methods

In this study, the PSNR value [27] and SSIM index [28] are used as referential evidence for image quality evaluation. The PSNR expressions are given below.

$$\begin{aligned} \mathrm{PSNR} &= 10 \times \log\left(\frac{255^2}{\mathrm{MSE}}\right) \\ \mathrm{MSE} &= \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x(i,j)-y(i,j)\right)^2 \end{aligned} \tag{10}$$

As a widely used objective measure for evaluating image quality, the mean square error (MSE) indicates the mean square deviation of each pixel value in the cover image and the stego image, and it is used to calculate the PSNR value. In general, the larger the PSNR value, the lesser is the distortion. PSNR is commonly used to objectively evaluate information hiding technologies.

SSIM is used for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as a reference. SSIM is designed to improve traditional methods such as PSNR and MSE [29]. The SSIM expression is as follows:

$$\mathrm{SSIM}(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{11}$$

where μ_x is the average of x; μ_y is the average of y; σ_x^2 is the variance of x; σ_y^2 is the variance of y; σ_{xy} is the covariance of x and y; $c_1 = (k_1L)^2$and $c_2 = (k_2L)^2$ are the two variables to stabilize the division with weak denominator; L is the dynamic range of the pixel values (typically this is $2^{\#\text{bits per pixel}} - 1$); $k_1 = 0.01$ and $k_2 = 0.03$ by default [29].

4.3 Analysis of experiment results

According to the block selection explained in Section 3, the pixel values are read in order in rows or columns, and the calculations are performed with every three pixel values as one group. The calculation results are summarized in Table 3, which shows that the number of differences of pixel values can lead to different results due to reading in rows or columns, and the results will influence the steganographic capacity of the entire digital image. Further, from Table 3, it can be seen that 1, 0, and − 1 appear most frequently among the differences of each digital image. However, according to the method proposed in this study, if steganography is conducted on the parts whose differences are "1 and 0" or "0 and − 1," the same pixel values may remain after steganography. For instance, if the information 1 is hidden in the pixel group whose difference is 0 or the information 0 is hidden in the pixel group whose difference is 1, the new difference 1 after steganography will be obtained in both scenarios, leading to incorrect ciphertext retrieval. Therefore, in this study, parts whose

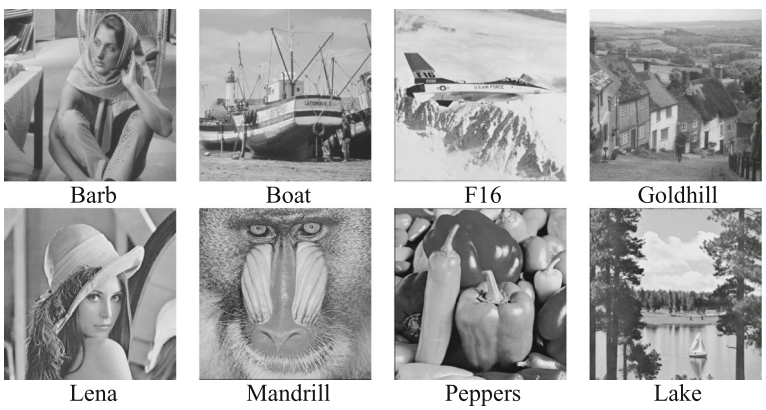


Fig. 7 Test images used in this study. Eight 512 × 512 grayscale test images that are widely used in the information hiding field were employed in this study

Fig. 8 Sample image of BOWS-2 image databases [26]. Sample image of BOWS-2 image databases. To verify the suitability of the hiding scheme for various image types, 9,074,512 × 512 grayscale images were selected from the BOWS-2 image databases as raw images

differences are 1 and − 1 are used for steganographic procedures.

According to the statistical results of Table 3, images with sums whose pixel values are 1 and − 1 read in rows and columns are compared (as shown in Table 4). The proposed PVO hiding scheme calculated the difference by row and column respectively and determined the direction of the data bit to be embedded by the higher sum of the differences. By judging the sum of the differences, the steganographic capacity can increase about 3.8–20.29%. Thus, the average steganographic capacity increment is 9.15%.

After ciphertext embedding in the used cover images according to the steganography steps proposed in this study, the steganographic capacity (bits), the capacity as a percentage of the image size (description in brackets), the PSNR values, and the SSIM index of PVO and PVOMM were compared. The experimental results are summarized in Table 5. Except for Mandrill, the steganographic capacity obtained by the steganographic method for each digital image is higher than that of PVO and PVOMM. The average steganographic capacity and the quality measured by the standard PSNR value of the digital images are compared to those of PVO. The steganographic capacity is improved by approximately 4600 bits while the PSNR value is reduced by approximately 1.5 dB. Compared to PVOMM, the steganographic capacity is improved by approximately 1200 bits while the PSNR value is improved by approximately 0.6 dB. It can be inferred that the method proposed in this study leads to the improvement in the steganographic capacity and digital image quality.

In Table 5, it can be seen that the steganographic capacity of Mandrill is the least. From its image characteristics, Mandrill is a digital image with a relatively complex texture and belongs to digital images with the least steganographic capacity in PVO and PVOMM. However, for the digital image F16, its steganographic capacity in PVO, PVOMM, and the method proposed in this study is maximum. It can be inferred from this result that F16 is a digital image with a smooth texture, similar tones, slight differences between neighboring pixel values, and no complex blocks or colors of different darkness degrees. More differences for steganography can be obtained in the case of similar extracted neighboring pixel values and steganography based on PVO. In other words, in digital images with smooth textures, steganography based on PVO can achieve a higher steganographic capacity and maintain a certain digital image quality compared to digital images with complex textures.

To prove that images belonging to complex or smooth textures affect the steganographic capacity of PVO, the statistical kurtosis coefficient was used to analyze the distribution of the digital image in a two-dimensional pixel block and a determination made as to whether the digital image contains a large number of identical pixels in the two-dimensional pixel block. Through threshold value judgment, the block is determined as a complex or smooth texture block. The threshold value of the kurtosis coefficient used in this study was 0.2. Blocks with a kurtosis coefficient greater than 0.2 represent smooth areas of image texture. Blocks with a kurtosis coefficient of less than 0.2 represent complex areas of image texture. In Table 5, it is clear that the steganographic capacity of Mandrill is the lowest and that of F16 is the highest. Therefore, this study divided these two images into 64-pixel blocks, respectively (as shown in Fig. 9), and calculated the kurtosis coefficient of the 64-pixel blocks. In Fig. 9 (a), it is clear that 20 groups of 64-pixel blocks of F16 had kurtosis values greater than 0.2. In Fig. 9 (b), it is clear that Mandrill's 64 groups of pixel blocks have no kurtosis values greater than 0.2. It can be seen in Fig. 9 (a) and (b) that F16 is a smooth texture image, so its steganographic capacity is relatively high; whereas, relatively speaking, Mandrill is a

Table 3 Statistical table of the number of differences of cover images

Difference	Barb		Boat		F16		Goldhill		Lena		Mandrill		Peppers		Lake	
	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns
− 2	12,192	10,637	13,622	13,359	12,648	13,376	11,271	11,801	14,574	13,225	6153	6543	13,278	13,012	10,735	10,926
− 1	*16,153*	*13,615*	*19,564*	*18,678*	*21,274*	*22,033*	*13,684*	*14,836*	*19,511*	*16,812*	*6566*	*7060*	*17,081*	*16,211*	*13,511*	*13,348*
0	19,251	15,412	24,329	22,192	34,013	33,863	15,160	16,450	24,992	19,402	6928	7570	19,459	18,699	15,232	15,051
1	*16,537*	*13,561*	*20,093*	*18,577*	*22,324*	*23,226*	*13,505*	*14,858*	*19,225*	*16,343*	*6748*	*7040*	*16,759*	*15,958*	*13,475*	*13,030*
2	12,198	10,596	13,651	13,475	12,695	13,309	10,885	11,823	14,519	13,194	6127	6630	13,469	13,125	10,764	10,315

Table 4 Statistical table of number increment of differences in cover images

Difference	Barb		Boat		F16		Goldhill		Lena		Mandrill		Peppers		Lake	
	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns
− 1	16,153	13,615	19,564	18,678	21,274	22,033	13,684	14,836	19,511	16,812	6566	7060	17,081	16,211	13,511	13,348
1	16,537	13,561	20,093	18,577	22,324	23,226	13,505	14,858	19,225	16,343	6748	7040	16,759	15,958	13,475	13,030
Sum	*32,690*	27,176	*39,657*	37,255	43,598	*45,259*	27,189	*29,694*	*38,736*	33,155	13,314	*14,100*	*33,840*	32,169	*26,986*	26,378
Increment (%)	20.29		6.45		3.81		9.21		16.83		5.90		5.19		2.30	

Difference	Lena		Mandrill		Peppers		Lake	
	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns	Read in rows	Read in columns
− 1	19,511	16,812	6,566	7,060	17,081	16,211	13,511	13,348
1	19,225	16,343	6,748	7,040	16,759	15,958	13,475	13,030
Sum	*38,736*	33,155	13,314	*14,100*	*33,840*	32,169	*26,986*	26,378
Increment (%)	16.83		5.90		5.19		2.30	

Table 5 Comparison of steganographic capacity, PSNR, and SSIM of the proposed method, PVO, and PVOMM

	PVO [13]			PVOMM [17]			Proposed		
	Capacity (bits)	PSNR (dB)	SSIM	Capacity (bits)	PSNR (dB)	SSIM	Capacity (bits)	PSNR (dB)	SSIM
Barb	27,882 (10.63%)	52.3103	0.999	29,912 (11.41%)	50.1862	0.999	32,690 (12.47%)	50.799	0.999
Boat	33,976 (12.96%)	52.6603	0.999	37,089 (14.14%)	50.4414	0.999	39,657 (15.13%)	51.0355	0.999
F16	37,795 (14.41%)	53.2083	0.999	43,363 (16.54%)	50.8986	0.999	45,259 (17.26%)	51.5886	0.999
Goldhill	25,992 (9.91%)	52.1817	0.999	28,205 (10.76%)	50.1091	0.999	29,694 (11.33%)	50.7501	0.999
Lena	31,523 (12.02%)	52.6284	0.999	36,120 (13.78%)	50.4357	0.999	38,736 (14.78%)	51.0517	0.999
Mandrill	12,966 (4.94%)	51.6118	0.999	14,277 (5.44%)	49.7203	0.999	14,100 (5.38%)	50.2712	0.999
Peppers	29,314 (11.18%)	52.3637	0.999	33,759 (12.88%)	50.2997	0.999	33,840 (12.91%)	50.8199	0.999
Lake	24,208 (9.23%)	52.123	0.999	27,443 (10.47%)	50.1007	0.999	26,986 (10.29%)	50.6709	0.999
Average	*27,957 (10.66%)*	52.386	0.999	*31,271 (11.93%)*	50.27	0.999	*32,620.25 (12.44%)*	50.87	0.999

complex texture image, so its steganographic capacity is low.

Rate-distortion curves of embedding bits using the proposed PVO with respect to test image quality are shown in Fig. 10. For Li's PVO, Chen's PVO, and the proposed PVO, we varied EC from 5000 bits to its maximum with a step size of 5000 bits. The figure shows that the capacity of the proposed method is superior to that of the state-of-the-art methods in most cases, while maintaining an acceptable PSNR, demonstrating the superiority of the proposed PVO hiding scheme.

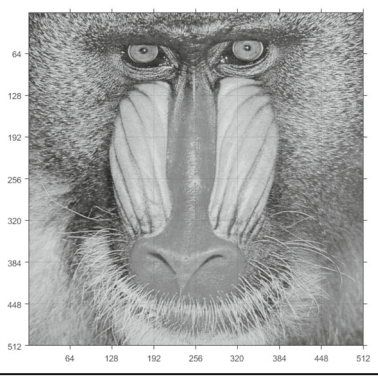
F16 divided into 64 pixel blocks

Kurtosis values of the 64 pixel blocks

0.0148	0.0167	0.0674	0.1854	0.0366	0.0113	0.0074	0.0075
0.114	**0.5616**	**0.3988**	**0.2548**	0.1227	**0.3017**	**0.5893**	**1.7783**
0.0064	0.0078	0.1692	**0.2285**	**0.5186**	**0.7384**	**0.2915**	**1.2648**
0.0063	0.0084	0.0072	0.0059	0.0063	0.007	0.0067	0.0109
0.0123	0.0087	0.01	0.0077	0.0101	0.0065	**0.5606**	**3.6405**
0.0064	0.009	0.0114	0.0122	0.0126	0.0107	0.0064	**2.7094**
0.9923	**1.8329**	0.0077	0.0102	0.0095	0.0081	0.0084	**2.0136**
0.3578	**1.9848**	**0.4081**	0.0399	0.023	0.0075	0.0133	0.0089

(a) F16

Mandrill divided into 64 pixel blocks



Kurtosis values of the 64 pixel blocks

0.01	0.0105	0.0118	0.0134	0.0123	0.0102	0.011	0.0101
0.0099	0.0101	0.0099	0.0113	0.0109	0.0101	0.0107	0.0097
0.0113	0.011	0.0085	0.0121	0.0087	0.0119	0.0113	0.0109
0.012	0.0116	0.0208	0.0115	0.0085	0.0125	0.0131	0.0158
0.012	0.0183	0.008	0.0111	0.0088	0.0072	0.0164	0.0266
0.0092	0.0095	0.0131	0.0222	0.0193	0.0142	0.0159	0.0238
0.0187	0.0121	0.0109	0.0245	0.0357	0.0103	0.0125	0.0269
0.0246	0.0137	0.0088	0.01	0.0097	0.0094	0.0138	0.0181

(b) Mandrill

Fig. 9 Kurtosis values of the 64-pixel blocks of F16 and Mandrill

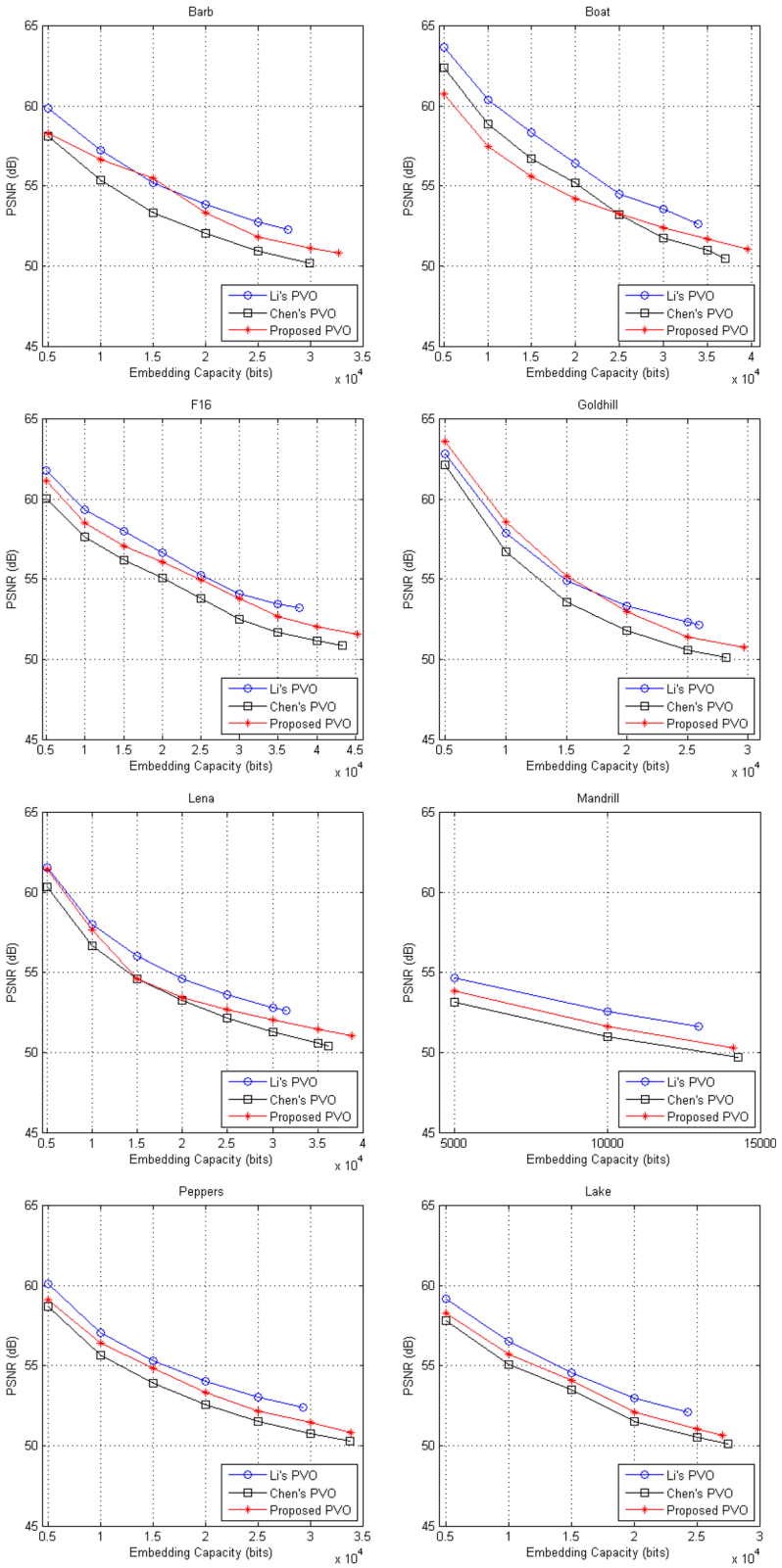


Fig. 10 Rate-distortion curves of embedding bits using the proposed PVO with respect to test image quality. Rate-distortion curves of embedding bits using the proposed PVO with respect to test image quality, including Barb, Boat, F16, Goldhill, Lena, Mandrill, Peppers, and Lake

Table 6 Experimental results of the proposed PVO, Li's PVO, and Chen's PVO for BOWS-2 image databases

	Proposed PVO	Li's PVO	Chen's PVO
Mean value of hiding capacity	*23,280.1*	17,730.7	20,990.9
Mean value of PSNR	52.9	*57.01*	55.12
Mean value of SSIM index	0.998	*0.999*	*0.999*

To assess the suitability of the proposed method to databases with different patterns, a further 9,074,512 × 512-pixel grayscale images were selected from the BOWS-2 [26] image databases as raw images. The proposed hiding scheme was then used to hide data and generate stego images in these images. The first row in Table 6 shows the mean value of the hiding capacity of the proposed PVO, Li's PVO, and Chen's PVO for the BOWS-2 image databases. The mean value of the hiding capacity of the proposed PVO is the best. The second and third rows in Table 6 show respectively the mean values of the PSNR and SSIM index for the BOWS-2 images. The mean values of the PSNR and SSIM index of the proposed PVO are inferior to those of Li's and Chen's PVO. The embedding capacity is higher compared to their methods while there is only a slight decrease in the SSIM value and a more severe one in the PSNR value. The results of a performance comparison with those of the PVO hiding schemes proposed by other researchers confirm that the proposed scheme has a higher capacity than the other methods while maintaining an acceptable PSNR, demonstrating the superiority of the proposed hiding scheme.

4.4 Security analysis against second-order SPAM features

Penvy et al. [30] presented second-order SPAM features for the detection of steganographic methods that embed in the spatial domain. To prove the security of the proposed method against the second-order SPAM features, 9074 cover images were retrieved from the BOWS-2 image database and the corresponding stego images of the proposed method were used to carry out the following experiment. The training image sets consisted of 4537 cover images and 4537 stego images for the proposed steganography algorithm. The remaining cover images and stego images were used for test image sets. The first step was to extract the 686 features of SPAM of training images. Furthermore, the stego images and cover images were given diverse labels. The purpose of the different labels used in the PNN training stage was to obtain the relationship between feature sets and classification categories. The second step was to use a more flexible classifier, PNN, which was employed to discriminate between cover images and the stego images. Finally, according to the classification results, the detection accuracy was calculated. The security of the proposed method against second-order SPAM features is presented in Table 7. From the SPAM detection results shown in Table 7, we can see that the accuracy, precision, recall, and F1 score were 53.54%, 52.4%, 77.6%, and 62.6%, respectively. Table 7 shows that the SPAM features cannot effectively identify the stego images generated using the proposed method and the cover images. This verifies that the stenography method proposed in this study is effective and robust against second-order SPAM features.

5 Conclusion

The evaluation of information hiding technologies involves comparison of the steganographic capacity and digital image quality. The steganography method proposed in this study can effectively improve steganographic capacity and digital image quality. A PSNR of above 50 dB or an SSIM value of 0.999 still indicates a very high image quality. As those values are achieved even with the maximum possible embedding capacity, this verifies that the stenography method proposed in this study is effective. The steganography method was applied after excluding the overflow blocks. According to the different steganographic images, scanning was conducted in rows or columns, and the differences were recorded. The proposed steganography method was applied to the images with a higher sum of those whose differences were 1 and − 1, through which the steganographic capacity was improved by 3.8–20.29%. The average steganographic capacity increment was approximately 9.15%. Furthermore, compared to PVO and PVOMM, the steganographic capacity was improved by nearly 1.78% and 0.51% while the PSNR value was reduced only by approximately 1.5 and 0.6, respectively, indicating that the differences of rows or columns dynamically selected in this study can effectively improve the steganographic capacity.

Table 7 Security of the proposed method against second-order SPAM features

TP	FN	TN	FP	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
3520	1017	1339	3198	*53.54*	*52.4*	*77.6*	*62.6*

Abbreviations
EC: Embedded capacity; HS: Histogram shifting; IPVO: Improved PVO; LM: Location map; LSB: Least-significant bit; MSE: Mean square error; PE: Prediction error; PEHS: Prediction error histogram shifting; PNN: Probabilistic neural network; PSNR: Peak signal-to-noise ratio; PVD: Pixel-value differencing; PVO: Pixel value ordering; PVOMM: PVO multi-pixel modification

Acknowledgements
This study was supported by the Ministry of Science and Technology of the Republic of China under Grant MOST 106-2221-E-606-002.

Funding
The initial stage of this research was funded by the Ministry of Science and Technology of the Republic of China under Grant MOST 106-2221-E-606-002, for the August 2017–July 2018 duration.

Availability of data and materials
The cover images and stego images used in the experiment, the code of the proposed PVO steganography and related experimental data in this study can be disclosed. Please contact author for data requests.

Authors' contributions
H-HL is the first author and the corresponding author. C-ML did some parts of the experiment. Both authors read and approved the final manuscript.

Competing interests
This study is for academic research and submission purposes only. The authors in this study declare that they have no competing interests.

Publisher's Note

Received: 27 September 2018 Accepted: 1 April 2019
Published online: 18 April 2019

References

1. F.-A.-P. Petitcolas, R.-J. Anderson, M.-G. Kuhn, Information hiding—a survey. Proc. IEEE **87**(7), 1062 (1999)
2. C.-K. Chan, M. Cheng, Hiding data in images by simple LSB substitution. Pattern Recogn. **37**, 469–474 (2004)
3. D.-C. Wu, W.-H. Tsai, A steganographic method for images by pixel-value differencing. Pattern Recogn. **24**, 1613–1626 (2003)
4. H.-C. Wu, N.-I. Wu, C.-S. Tsai, M.-S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEEE Proc. Vision Image Signal Process. **152**(5), 611–615 (2005)
5. Z. Ni, N. Y-Q Shi, W.S. Ansari, Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol. **16**(3), 354–362 (2006)
6. J.-H. Hwang, J.-W. Kim, J.-U. Choi, A reversible watermarking based on histogram shifting. Lect. Notes Comput. Sci **4283**, 348–361 (2006)
7. M. Fallahpour, M.-H. Sedaaghi, High capacity lossless data hiding based on histogram modification. IEICE Electron. Expr. **4**(7), 205–210 (2007)
8. H.-W. Tseng, C.-P. Hsieh, Reversible data hiding based on image histogram modification. Imaging Sci. J. **56**(5), 271–278 (2008)
9. X. Zhang, Reversible data hiding in encrypted image. IEEE Signal Proc. Let. **18**(4), 255–258 (2011)
10. C. Qin, C. Chang, Y. Chiu, A novel joint data-hiding and compression scheme based on SMVQ and image inpainting. IEEE Trans. Image Process. **23**(3), 969–978 (2014)
11. S. H Huang, Y.L. Li, in *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Piraeus*. Multi-level reversible data hiding with pyramidal structure (2012), pp. 234–237
12. W. Hong, T.-S. Chen, C.-W. Shiu, Reversible data hiding for high quality images using modification of prediction errors. J. Syst. Softw. **82**(11), 1833–1842 (2009)
13. P. Tsai, Y.-C. Hu, H.-L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process. **89**(6), 1129–1143 (2009)
14. K.-S. Kim, M.-J. Lee, H.-Y. Lee, H.-K. Lee, Reversible data hiding exploiting spatial correlation between sub-sampled images. Pattern Recogn. **42**(11), 3083–3096 (2009)
15. X. Li, J. Li, B. Li, B. Yang, High fidelity reversible data hiding scheme and prediction-error expansion. Signal Process. **93**(1), 198–205 (2013)
16. F. Peng, X. Li, B. Yang, Improved PVO-based reversible data hiding. Digital Signal Process. **25**, 255–265 (2014)
17. X. Qu, H.-J. Kim, Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding. Signal Process. **111**, 249–260 (2015)
18. X. Wang, J. Ding, Q. Pei, A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition. Inf. Sci. **310**, 16–35 (2015)
19. Y.-T. Chen, C.-S. Tsai, H.-C. Wu, in *Master's thesis, National Chung Hsing University, R.O.C.* A study on high capacity reversible information hiding using pixel-value-ordering and multi-pixel modification (2016)
20. A. Westfeld, A. Pfitzmann, in *Proceedings of the 3rd International Workshop on Information Hiding*. Attacks on steganographic systems (1999), pp. 61–75
21. J. Fridrich, M. Goljan, D. R, Detecting LSB steganography in color and gray-scale images. IEEE Multimedia **8**(4), 22–28 (2001)
22. X. Zhang, S. Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recogn. Lett. **25**(3), 331–339 (2004)
23. W.-C. Kuo, Y.-H. Lin, Y.-Z. Huang, Y.-C. Lee, in *Proceedings of the 7th Conference on Information Technology and Applications in Outlying Islands*. On the security of histogram-based reversible data hiding (2008), pp. 205–208
24. C.-L. Liu, H.-H. Liu, Reliable detection of histogram shift-based steganography using payload invariant features. Appl. Mech. Mater. **284**, 3517–3521 (2012)
25. C.-F. Lee, C.-C. Chang, J.-J. Li, Y.-H. Wu, in *2016 Nicograph International*. A survey of reversible data hiding schemes based on pixel value ordering (2016), pp. 68–74
26. Bows-2 image database. http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=credits. Accessed on 10 May 2015
27. A.-M. Eskicioglu, P.-S. Fisher, Image quality measures and their performance. IEEE Trans. Commun. **43**(12), 2959–2965 (1995)
28. Z. Wang, A.-C. Bovik, H.-R. Sheikh, E.-P. Simoncelli, Image quality assessment: From error visibility to structural similarity. IEEE Trans. Image Process. **13**(4), 600–612 (2004)
29. Structural similarity. https://en.wikipedia.org/wiki/Structural_similarity. Accessed on 20 Nov 2018
30. T. Pevný, P. Bas, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix. IEEE Trans. Inf. Forensic Secur. **5**(2), 215–224 (2010)