EURASIP Journal on Advances in Signal Processing

RESEARCH Open Access

Statistical feature-based steganalysis for pixel-value differencing steganography

Wen-Bin Lin[1], Tai-Hung Lai[2*] and Ko-Chin Chang[3]

*Correspondence: sudolai@gmail.com
[2] Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan County, Taiwan, ROC
Full list of author information is available at the end of the article

Abstract

Pixel-value differencing (PVD) steganography is a popular spatial domain technology. Several PVD-based studies have proposed extended PVD steganography methods. The majority of these studies have verified their security against the regular-singular (RS) analysis. However, RS analysis is aimed at the feature of the least significant bit substitution method, which is relatively less significant for PVD steganography. The pixel difference histogram (PDH) is generally utilized to attack PVD steganography. If the embedding capacity is high, then the features on the PDH are evident; otherwise, the features are less obvious. In this paper, we propose a statistical feature-based steganalysis technique for the original PVD steganography. Experimental results demonstrate that, compared with existing steganalysis technique with weighted stego-image (WS) method, the proposed method effectively detects PVD steganography at low embedding ratios, such that there is no need of using the original embedding parameters. Furthermore, the accuracy and precision of the method are better than those of existing PVD steganalysis techniques. Therefore, the proposed method contributes to the security analysis of the original PVD steganography as an alternative to the commonly used RS, PDH and WS attack techniques.

Keywords: Pixel-value differencing, Steganalysis, Steganography

1 Introduction

Cryptography and steganography are used to protect and secure information. Encryption algorithms protect secret data by converting it into unreadable data; however, such unreadable and incomprehensible data are likely to draw the attention of criminals. Steganography can conceal data in carriers without changing the original data. Common carriers include videos, audios, texts, and images. Compared with other carriers, digital images have considerable amount of redundant space. Therefore, digital images are commonly used for steganography and are called cover images (before embedding secret messages); similarly, images with embedded messages are called stego images. Steganography techniques can be categorized into spatial and frequency domains. In terms of image quality, the embedding capacity in the spatial domain is higher than that in the frequency domain. Therefore, the spatial domain is suitable for a large number of embedded messages. In the spatial domain, the least significant bit (LSB) substitution steganography [1], proposed in 1996, is the most popular steganography technique.

© The Author(s), 2021. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Here, the LSB bit of a pixel value is directly substituted by secret bitstreams. However, LSB substitution steganography can be detected using regular-singular (RS) analysis [2].

Pixel-value differencing (PVD) steganography [3] was developed based on the edge areas in an image; it can conceal more secret messages compared to those in smooth areas. Based on this principle, PVD steganography determines the amount of messages to be embedded depending on the value of the difference between adjacent pixels. Although this method provides a high embedding capacity and invisibility, it creates a step-like shape in the pixel difference histogram (PDH), and embedded messages may be detected. A modified PVD (MPVD) steganography was proposed by Zhang et al. [4], which dynamically generates the PVD interval range to improve security.

In recent years, many scholars have proposed PVD-based methods and have verified their safety via RS analysis. For instance, a hybrid method was proposed [5] using LSB steganography in smooth areas and PVD steganography in edge areas. In other studies [6–15], the combination of PVD and LSB techniques has been proposed to obtain a large embedding capacity. In addition, other hybrid methods have been proposed to offer a high embedding capacity, such as PVD combined with the side-match method [16] or exploiting modification directions [17, 18].

Because PVD steganography does not make full use of edge areas, a tri-way PVD (TPVD) steganography was proposed by Chang et al. [19], which utilizes three different directional edges to improve the embedding capacity. To achieve a higher embedding capacity, many studies [20–25] used PVD with LSB techniques in multi-directional edges. Afterward, to provide a good image quality, a PVD steganography technique using the modulus function (MFPVD) was proposed by Wang et al. [26]. This method utilizes the concept of congruence modulo to adjust the remainder of two consecutive pixels and match the message value. Many scholars have utilized this concept to formulate related studies [27–34].

With the popularity of steganography, a field of steganalysis was generated that is aimed at detecting the presence of embedding data in a stego image. Recently, most studies on steganalysis have mainly used machine learning and deep learning methods [35–39]. Many steganalysis techniques with multidimensional features have been proposed to improve the performance of detection; however, these techniques utilize multiple complex processes and computational resources. In addition, steganalysis schemes can be classified into universal or specific. The universal steganalysis scheme is designed to detect embedding messages regardless of the steganography technique used, such as deep learning methods. In contrast, specific steganalysis scheme aims to detect known steganography.

The steganalysis of the original PVD steganography [3] was first proposed by Zhang et al. [4], which made the step effects of the PDH and detected embedding messages. In 2019, Zhang et al. [40] proposed PVD noise steganalysis with weighted stego image (WS) steganalysis to detect the embedding capacity of the original PVD steganography, but the original steganography parameters need to be obtained. MPVD steganography [4] overcomes the step effects of the original PVD steganography, but it was detected through a one-more-time embedding [41–43] and revealed the features of the difference between before and after embedding messages.

Table 1 Type 1 of the PVD interval classification table

k	R_k	l_k	u_k	w_k	n
1	[0, 7]	0	7	8	3
2	[8, 15]	8	15	8	3
3	[16, 31]	16	31	16	4
4	[32, 63]	32	63	32	5
5	[64, 127]	64	127	64	6
6	[128, 255]	128	255	128	7

In addition, the steganalysis of TPVD steganography was proposed by Zaker et al. [44], which utilized the vulnerability from the PDH of stego images under TPVD steganography. Subsequently, because the embedding process of MFPVD steganography [26] generates fluctuations and growing abnormalities, the asymmetry on the PDH is created. The steganalysis of MFPVD [26] was proposed by Joo et al. [45], which utilizes these features to detect the embedding messages.

The above PVD-based studies are extensions of the traditional PVD steganography techniques [3]. These techniques have only verified their security against RS analysis. However, RS analysis is aimed at the feature of the LSB substitution method [2], which is relatively less significant for PVD steganography [3]. In addition, the PDH method [4] and WS technique [40] are commonly used to detect the original PVD steganography [3]. In existing studies, the PDH method has been commonly used for PVD-based steganalysis; however, its effectiveness is limited in low embedding ratios.

Therefore, we propose a statistical feature-based method for steganalysis of the original PVD steganography [3]. Compared with the state-of-the-art steganalysis [40], the proposed method is more accurate and precise at low embedding ratios and can be performed without obtaining the original embedding parameters.

This article is organized as follows: Sect. 2 describes the related techniques. Section 3 details our proposed steganalysis of the original PVD steganography. Section 4 presents the experimental results and discussion. Finally, Sect. 5 shows the conclusions.

2 Related works

2.1 PVD steganography

PVD steganography was proposed by Wu et al. [3]. The concept is based on small changes in smooth areas, which are more easily detected by the human eye compared to the edge areas. Therefore, when secret data are embedded, a large change between the pixels in the edge area can be applied, thereby allowing a large amount of secret data to be embedded in the edge area. The embedding process is described as follows:

First, cover images divided every two consecutive and non-overlapped pixels in a zigzag manner into the embedding block. We assume that the values of pixels in the embedding blocks are p_i and p_{i+1}, respectively, and the difference value d between the two pixels in each block is computed as $p_{i+1} - p_i$.The difference value d lies between -255 and 255. Based on the embedding capacity and image quality requirements, two types of PVD interval classification tables are designed (i.e., Tables 1 and 2). Tables 1 and 2 indicate the absolute value of the difference, which is divided into many continuous ranges

Table 2 Type 2 of the PVD interval classification table

k	R_k	l_k	u_k	w_k	n
1	[0, 1]	0	1	2	1
2	[2, 3]	2	3	2	1
3	[4, 7]	4	7	4	2
⋮	⋮	⋮	⋮	⋮	⋮
12	[128, 191]	128	191	64	6
13	[192, 255]	192	255	64	6

R_k, where the interval index value, lower bound, upper bound, and width of the range are defined as k,l_k,u_k, and w_k, respectively. The width of the range is a power of 2, and the value is $w_k = u_k - l_k + 1$. The number of embedding bits n is determined by the width of the PVD interval, as shown in Eq. (1):

$$n = \log_2 (w_k) \tag{1}$$

Table 1 indicates type 1 of the PVD interval classification table. The width of each PVD interval is large, which can embed a large number of bits and is commonly used in steganography and steganalysis. Table 2 indicates type 2 of the PVD interval classification table. The width of each PVD interval is small, which embeds a small number of bits; however, the quality of the stego image is better. Subsequently, the secret bits n are converted into a decimal value b, and the new difference value d' is calculated as follows:

$$d' = \begin{cases} l_k + b, & \text{if } d \geq 0 \\ -(l_k + b), & \text{if } d < 0 \end{cases} \tag{2}$$

Let the values of pixels in the stego image be p'_i and p'_{i+1}. The embedding procedure is presented as follows:

$$\left(p'_i, p'_{i+1}\right) = \begin{cases} \left(p_i - \left\lceil \dfrac{d' - d}{2} \right\rceil, p_{i+1} + \left\lfloor \dfrac{d' - d}{2} \right\rfloor\right), \\ \text{if } d \text{ is odd,} \\ \\ \left(p_i - \left\lfloor \dfrac{d' - d}{2} \right\rfloor, p_{i+1} + \left\lceil \dfrac{d' - d}{2} \right\rceil\right), \\ \text{if } d \text{ is even} \end{cases} \tag{3}$$

where $\lceil\ \rceil$ is the ceiling function to round toward infinity and $\lfloor\ \rfloor$ is the floor function to round toward minus infinity.

Overall, the secret bits are embedded in the PVD of each pixel pair through PVD steganography, which is not the same as the LSB substitute steganography [1].

2.2 WS steganalysis

Zhang et al. [40] proposed a WS steganalysis method for the original PVD steganography [3]. In this method, the feature of the stego noise in sum value images is similar to that of LSB substitution steganography [1]. This method only involves normal embedding blocks, which are denoted by A. The maximal embedding rate in bits per pixel is presented in Eq. (4):

$$r_{\max} = \frac{|A|}{2N} \sum_{k \in Z6} P(\left|d_i\right| \in R_k | i \in A) \log_2(w_k), \tag{4}$$

where N is the number of pixel pairs.

The estimator of a cover image is denoted as $\hat{c}$, and it is obtained using a local linear predictor with fixed forms, as shown in Eq. (5).

$$T = \begin{bmatrix} -\frac{1}{4} & \frac{1}{2} & -\frac{1}{4} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{4} & \frac{1}{2} & -\frac{1}{4} \end{bmatrix} \tag{5}$$

Then, the residuals r_i are calculated as follows:

$$r_i = (s_i - \tilde{s}_i)(s_i - \hat{c}_i), \; i \in A, \tag{6}$$

where $\tilde{s}_i$ indicates the flipped LSB value of the stego pixel.

If σ^2 is the variance of estimator $\hat{c}_i$, then the weighted function is calculated as follows:

$$w(\sigma^2) = \frac{1}{\lambda + \sigma^2}, \tag{7}$$

where λ is a constant (λ=5) [40].

WS residuals in the sum value of the stego image are calculated, and the LSB substitution embedding rate is estimated using Eq. (8).

$$\hat{p} = \frac{2 \sum\limits_{i \in \mathrm{A}} w(\sigma_i) r_i}{\sum\limits_{i \in A} w(\sigma_i)}, \tag{8}$$

where $\hat{p}$ is used to estimate a PVD embedding rate as follows:

$$\hat{r} = r_{\max}\hat{p} = \frac{2r_{\max} \sum\limits_{i \in \mathrm{A}} w(\sigma_i) r_i}{\sum\limits_{i \in A} w(\sigma_i)} \tag{9}$$

If $\hat{r} < 0$, then $\hat{r}$ must be corrected to be zero. However, if $\hat{r} > r_{\max}$, then $\hat{r}$ must be corrected to be $r_{\max}$. This method indicates that estimators are sensitive to the sample size and relative embedding ratios. Therefore, the performance of the best WS estimator is employed according to the embedding parameters.

3 Proposed steganalysis technique

In this section, we describe our method for steganalysis of the original PVD steganography [3]. This method involves two phases: the first phase is the drawback analysis of PVD steganography in Sect. 3.1, and the second phase is the detection of PVD steganography based on the drawbacks presented in Sect. 3.2. The difference value between pixel pairs is denoted as x. The original images with 1,000 images are used from the Break Our Steganographic System (BOSS) database [46] with 10,000 grayscale image sets that

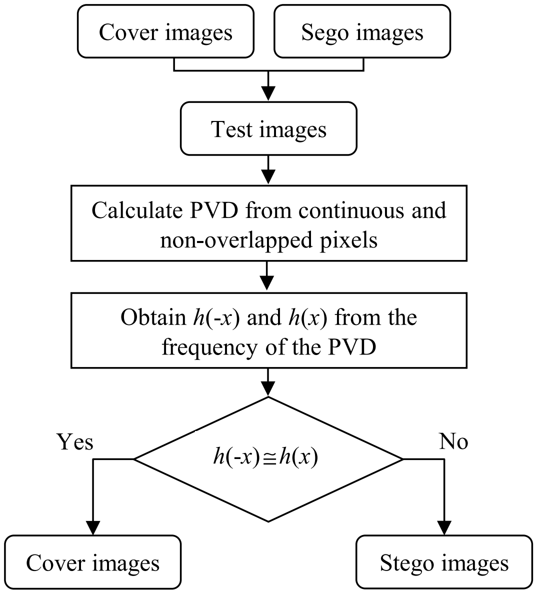
Cover images
Sego images
Test images
Calculate PVD from continuous and non-overlapped pixels
Obtain $h(-x)$ and $h(x)$ from the frequency of the PVD
$h(-x) \cong h(x)$
Yes
No
Cover images
Stego images

Fig. 1 Block diagram of the analytic process

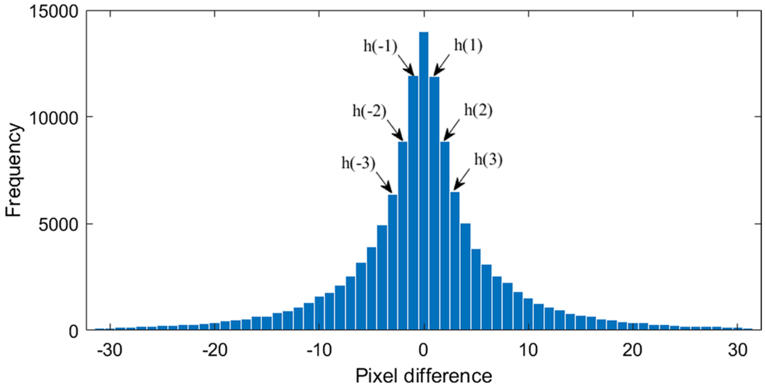

Fig. 2 Histogram of the pixel differences of a cover image

are 512 × 512 pixels in size. The histograms of PVD in the cover and stego images are defined as $h(x)$ and $h'(x)$, respectively, and the bin range in the histogram is from − 32 to 32.

3.1 Analyses of PVD steganography

In this section, we analyze the features of PVD distribution between the cover image and stego image and distinguish the difference between the original image and hidden image. In this study, the secret bitstreams were randomly generated with zeroes and ones and are approximately uniformly distributed. The stego images were embedded messages from the PVD steganography [3]. The analytical process is proposed, as shown in Fig. 1.

First, stego images were created using type 1 of the PVD interval classification table of PVD steganography [3] (i.e., Table 1) with an embedding ratio of 100%. The test images were a set of the cover and stego images. The histogram of PVD was executed

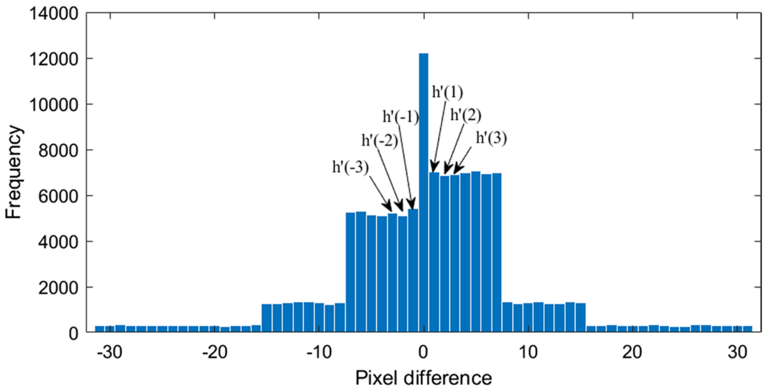

Fig. 3 PDH using PVD steganography with an embedding ratio of 100% (type 1 of the PVD interval)

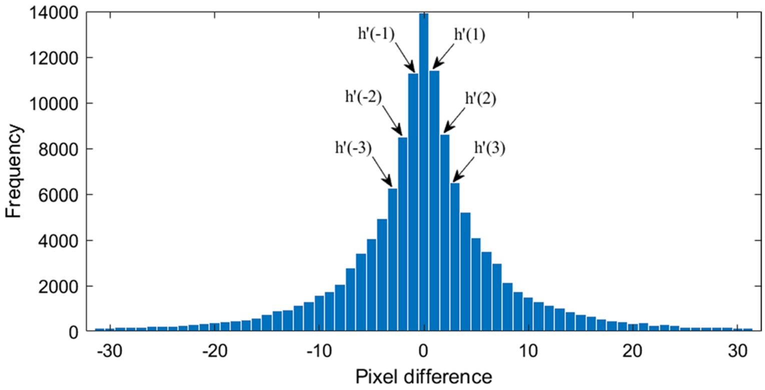

Fig. 4 PDH using PVD steganography with an embedding ratio of 10% (type 1 of the PVD interval)

through numerous experiments. Figures 2 and 3 show the histogram of PVD before and after embedding, respectively. The high correlation between the original adjacent pixels makes the frequency of PVD in the smooth area greater than that in the edge area. Therefore, the PDH of the original image follows a Laplacian distribution [47], as shown in Fig. 2.

When the histogram of PVD in the cover image follows a Laplacian distribution, the midpoints of the top edges of the rectangles in the histogram are connected by a smooth curve, which is similar to a bell curve. $h(1)$ and $h(2)$ are similar to $h(-1)$ and $h(-2)$, respectively, and so on, for other integers. Furthermore, the process of embedding messages changes the correlation between adjacent pixels, and the PDH of the stego image exhibits a step-like shape and left–right asymmetry, as shown in Fig. 3, where $h'(1)$ and $h'(2)$ are greater than $h'(-1)$ and $h'(-2)$, respectively, and so on, for other integers. When the test image is a stego image with an embedding ratio of 10%, the features of the step-like shape and left–right asymmetry are not evident on the PDH, as shown in Fig. 4.

Figures 5 and 6 show the PDH of a stego image using type 2 of the PVD interval classification table of PVD steganography (i.e., Table 2) with embedding ratios of 100% and 10%, respectively. If a stego image has an embedding ratio of 100%, then the histogram of PVD exhibits a step-like shape and slightly left–right asymmetry, as shown in Fig. 5.

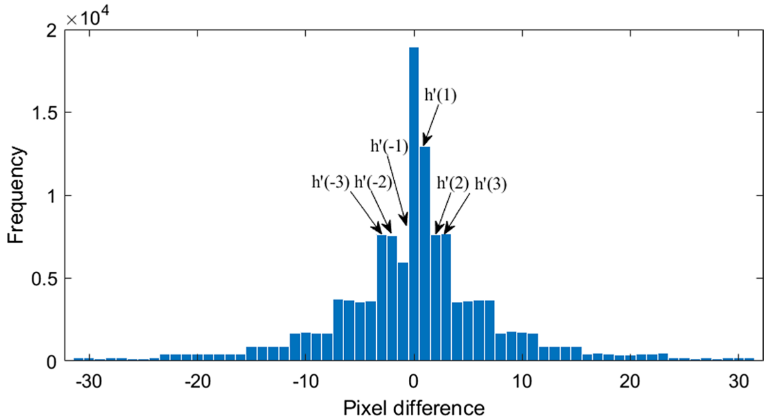

Fig. 5 PDH using PVD steganography with an embedding ratio of 100% (type 2 of the PVD interval)

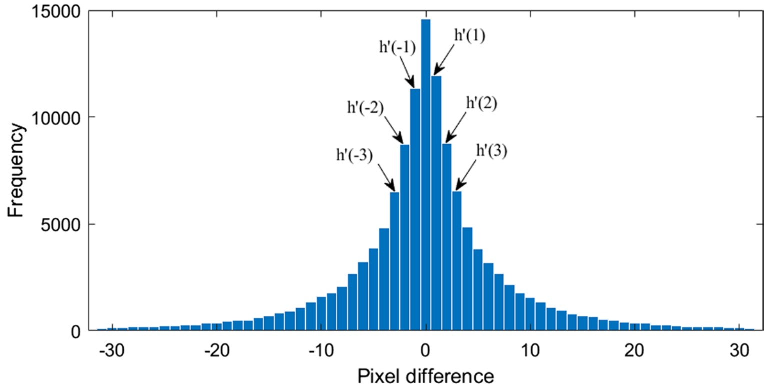

Fig. 6 PDH using PVD steganography with an embedding ratio of 10% (type 2 of the PVD interval)

If a stego image has an embedding ratio of 10%, then the PVD histogram has an unclear step-like and left–right asymmetry, as shown in Fig. 6.

3.2 Steganalysis of the PVD technique

When an embedding ratio is low, the feature on the PDH method is not evident. Therefore, using a feature of the difference between the cover and stego images, we propose a method based on the statistical feature. The difference value between pixel pairs and the frequency of PVD are denoted as x and $h(x)$, respectively. If a suspicious image is a cover image, then the probability of $h(x)$ and $h(-x)$ will be approximately similar based on the previous analysis mechanism.

In real scenarios, a suspicious image cannot easily be confirmed as a cover image. Therefore, we can compare the difference between the theoretically expected frequency and observed frequency. When the secret messages are embedded into an image, the LSB values of a pixel are only changed, and the sum of the frequencies of $h(x)$ and $h(-x)$ is not changed. Therefore, the theoretically expected frequency can be obtained from any randomly obtained suspicious image, and the original image is not required.

We assume that the suspicious image is a cover image. In addition, we use significant features and a small number of test pairs as the detection range to effort the efficiency of detection. Let X be the set of test pairs:

$$X_i = \{[h(-x_i), h(x_i)]\}, \tag{10}$$

where $i = 1, 2, \ldots, 7$.

The proposed method focuses on the similarity between the theoretically expected frequency and observed frequency, where the theoretically expected frequency is the average value of the two frequencies in any differences of the pixel pairs. We detect the degree of variability of test pairs as follows:

$$F = \frac{1}{n}\sum_{i=1}^{7}\frac{(X_i - E(X_i))^2}{E(X_i)}, \tag{11}$$

where n is the number of test pairs.

If the suspicious image is a cover image, then the frequency of the theoretically expected is similar to the frequency of observations, and the F value will be very small. On the contrary, the F value of a stego image is a very large value. We can obtain an appropriate threshold value through many experiments to distinguish between cover and stego images. If the suspicious image is a cover image, then the F value is less than the threshold value; otherwise, the suspicious image is a stego image (Fig. 7).

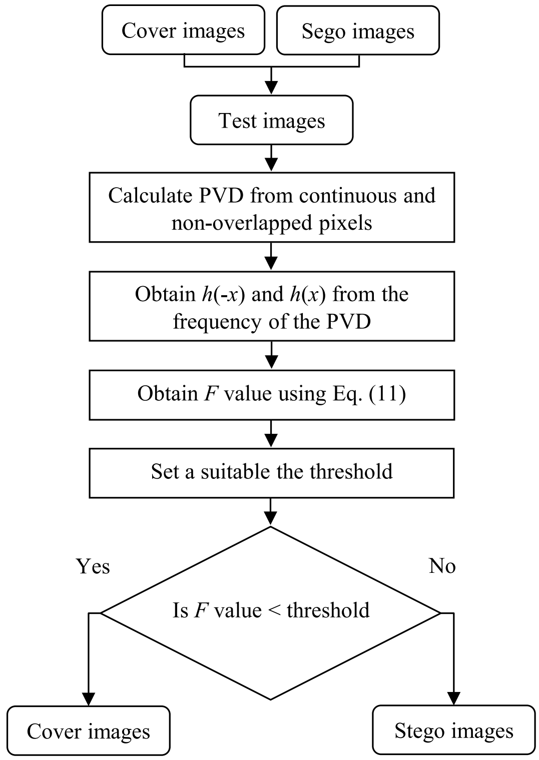
Cover images
Sego images
Test images
Calculate PVD from continuous and non-overlapped pixels
Obtain h(-x) and h(x) from the frequency of the PVD
Obtain F value using Eq. (11)
Set a suitable the threshold
Yes
No
Is F value < threshold
Cover images
Stego images

Fig. 7 Flowchart of the proposed technique

4 Experimental results and discussion

In this section, we discuss the extensive experiments conducted to validate the proposed method. The experimental environment was implemented using MATLAB R2018a on an Intel Core i5-8250U with 8 GB of RAM. Secret bitstreams were simulated with the MATLAB random number generator. We considered the detection of steganalysis as the binary classification problem with which to measure the effectiveness of the proposed method. The prediction of whether the suspicious image is a stego image or cover image is divided into four scenarios:

(1) True positive (TP): a stego image is correctly classified as a stego image.
(2) False negative (FN): a stego image is incorrectly classified as a cover image.
(3) True negative (TN): a cover image is correctly classified as a cover image.
(4) False positive (FP): a cover image is incorrectly classified as a stego image.

In general, the two criteria for validating steganalysis techniques are accuracy and precision. The proposed method was evaluated based on these criteria to verify the detection performance. The accuracy metric represents the proportion of correctly predicted classes. The precision metric represents the proportion of positive predictions that are correct. The accuracy and precision should be as high as possible, which are calculated using Eqs. (12) and (13), respectively.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \tag{12}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{13}$$

4.1 Effectiveness of the proposed method for various embedding ratios

The experiment process was divided into two cases on the basis of the types of PVD interval classification table from the original PVD steganography [3] (i.e., Tables 1 and 2). First, we evaluated our proposed method in type 1 of the PVD interval classification table (i.e., Table 1). The cover images are grayscale images, which were taken from the BOSS [46] database. The test was randomly performed on 1000 images selected from 10,000 images that were 512 × 512 pixels in size.

In the first experiment, we evaluated our proposed method for low embedding ratios ranging from 10 to 50%. In addition, the method was evaluated at an embedding ratio of 100%. We further discussed the results obtained from our proposed technique with embedding ratios of 100% and 10%. A comparison of the distribution of the cover images with that of stego images for embedding ratios of 100% and 10% (Figs. 8 and 9, respectively) indicates that the cover and stego images were clearly distinguished. When the suggested images are cover images, the *F* value is very low. A suitable threshold (1.4) of the *F* value was obtained through the experiments that were distinguished effectively between the cover and stego images.

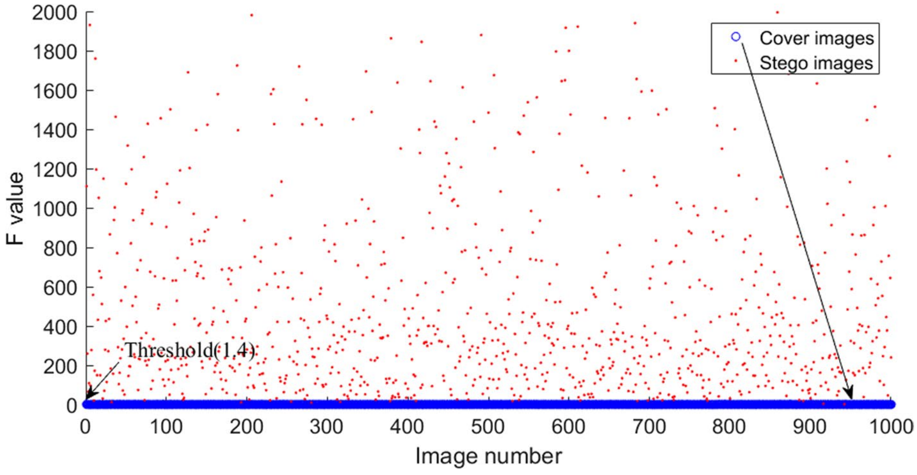

Fig. 8 Distribution of the cover and stego images at an embedding ratio of 100% (type 1 of the PVD interval)

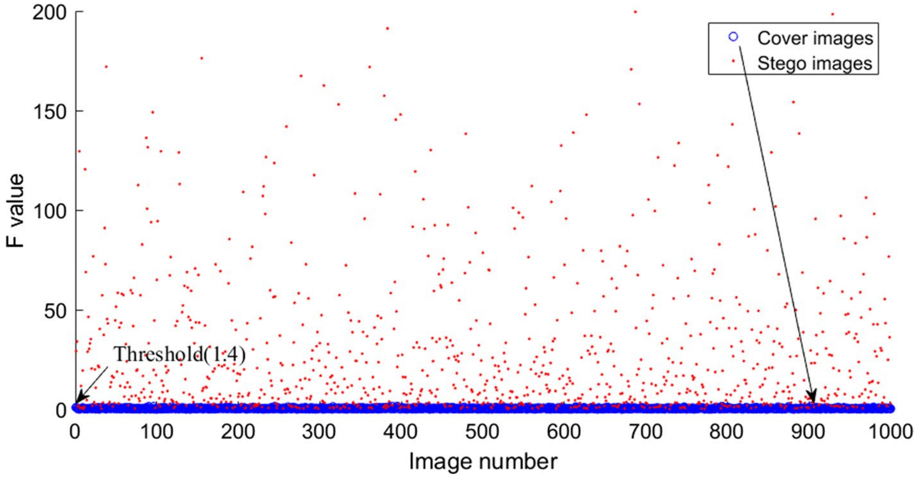

Fig. 9 Distribution of the cover and stego images at an embedding ratio of 10% (type 1 of the PVD interval)

Table 3 Results of the proposed technique (type 1 of the PVD interval)

Embedding ratio (%)	True positive	False negative	True negative	False positive	Accuracy
10	885	115	998	2	0.942
20	961	39	998	2	0.980
30	990	10	998	2	0.994
40	1000	0	998	2	0.999
50	1000	0	998	2	0.999
100	1000	0	998	2	0.999

Table 3 indicates that the accuracy of the proposed method is high, with more than 90% of the samples correctly identified, even at low embedding ratios.

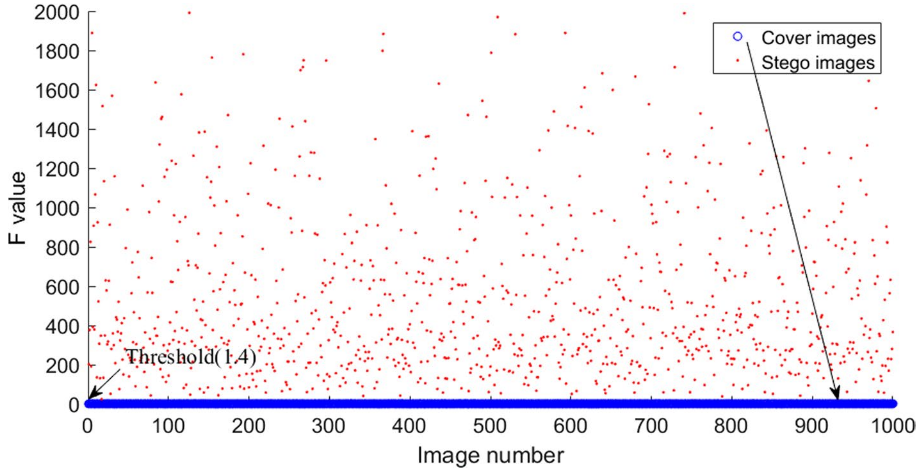

Fig. 10 Distribution of the cover and stego images with an embedding ratio of 100% (type 2 of the PVD interval)

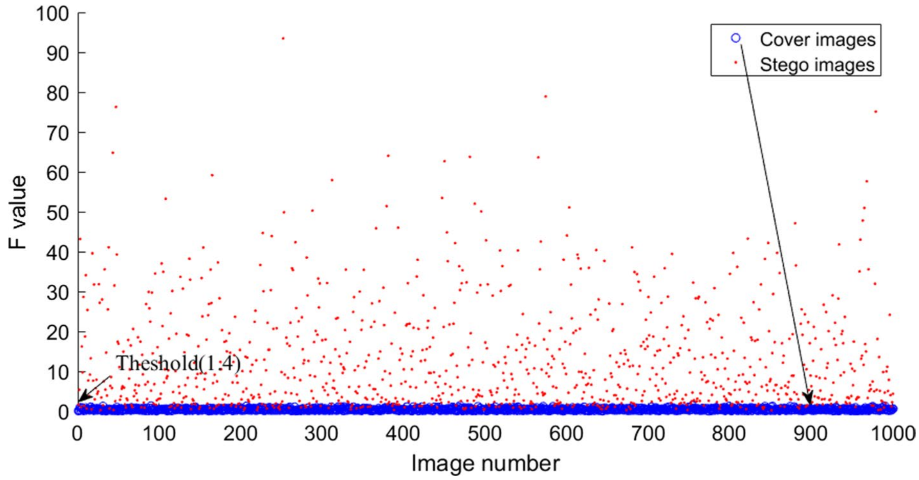

Fig. 11 Distribution of the cover and stego images with an embedding ratio of 10% (type 2 of the PVD interval)

In the second experiment, we used the same method in type 2 of the PVD interval classification table (i.e., Table 2) to evaluate our proposed method. A comparison of the distribution of the cover images with that of stego images for embedding ratios of 100% and 10% (Figs. 10 and 11, respectively) indicates that the cover and stego images were also distinguished clearly. For a better explanation of the threshold, we set the y-axis of Fig. 11 limits to range from zero to three, as shown in Fig. 12, where the appropriate threshold value is obtained through many experiments to distinguish between cover and stego images.

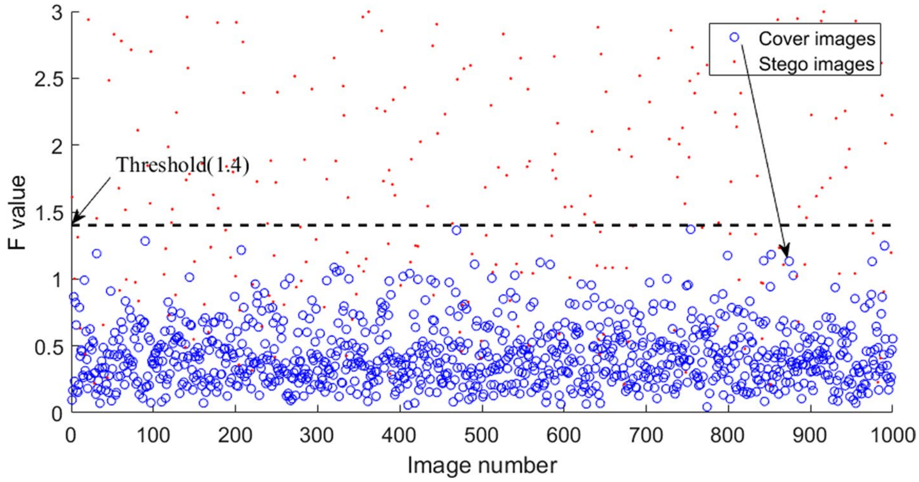

Fig. 12 The threshold of the *F* value with an embedding ratio of 10% (type 2 of the PVD interval)

Table 4 Results of the proposed technique (type 2 of the PVD interval)

Embedding ratio (%)	True positive	False negative	True negative	False positive	Accuracy
10	890	110	998	2	0.944
20	978	22	998	2	0.988
30	994	6	998	2	0.996
40	998	2	998	2	0.998
50	998	2	998	2	0.998
100	999	1	998	2	0.999

If the suspicious image is a cover image, then the *F* value is less than the threshold; otherwise, the suspicious image is a stego image. Overall, the proposed threshold value is applicable to various PVD interval types and embedding ratios.

Table 4 indicates that the accuracy of the proposed method is also high, with more than 90% of the samples correctly identified, even at low embedding ratios.

4.2 Comparative analysis with state-of-the-art techniques

To prove the superiority of the proposed steganalysis technique, we compared the performance of our proposed method with that of the state-of-the-art method [40] using various types of images and embedding ratios. The cover images, which are grayscale images, were taken from the BOSS [46] and Break Our Watermarking System 2 (BOWS2) [48] image databases, respectively. Tests were randomly performed on 1,000 images selected from the 10,000 images that were 512 × 512 pixels in size. Stego images were generated from the common type 1 of PVD interval classification table from PVD steganography [3] (i.e., Table 1).

In Zhang et al. [40], the best option for the WS estimator for the PVD steganalysis technique was proposed. We conducted the parameters of a local linear predictor with the usualness and best-estimated performance. The estimator value of a cover image should be zero. Therefore, we assumed the threshold to be zero.

Table 5 Comparison of the accuracy of methods for the BOSS image database

Embedding ratio (%)	Proposed method	Zhang et al.'s method [40]
10	0.942	0.742
20	0.980	0.751
30	0.994	0.757
40	0.999	0.757
50	0.999	0.756
100	0.999	0.757

Table 6 Comparison of the precision of methods for the BOSS image database

Embedding ratio (%)	Proposed method	Zhang et al.'s method [40]
10	0.998	0.666
20	0.998	0.671
30	0.998	0.673
40	0.998	0.673
50	0.998	0.673
100	0.998	0.673

Table 7 Comparison of the accuracy of methods for the BOWS2 image database

Embedding ratio (%)	Proposed method	Zhang et al.'s method [40]
10	0.936	0.758
20	0.982	0.769
30	0.996	0.769
40	0.998	0.770
50	0.999	0.770
100	0.999	0.771

Table 8 Comparison of the precision of methods for the BOWS2 database image

Embedding ratio (%)	Proposed method	Zhang et al.'s method [40]
10	0.997	0.680
20	0.997	0.685
30	0.997	0.685
40	0.997	0.686
50	0.997	0.686
100	0.997	0.686

Using 1,000 images, we compared the detection performance of the proposed method with that of the state-of-the-art technology [40] in terms of accuracy and precision. A comparison of the results with respect to accuracy and precision is presented in Tables 5, 6, 7 and 8. Tables 5, 6, 7 and 8 indicate that the accuracy and precision of the proposed method are high, with more than 90% of the samples correctly identified, even at low embedding ratios.

Table 9 Comparison of the accuracy for the UCID database images

Embedding ratio (%)	Proposed method	Zhang et al.'s method [40]
10	0.919	0.716
20	0.975	0.725
30	0.996	0.728
40	0.999	0.730
50	0.999	0.729
100	0.999	0.730

Table 10 Comparison of the precision for the UCID database images

Embedding ratio (%)	Proposed method	Zhang et al.'s method [40]
10	0.998	0.643
20	0.998	0.647
30	0.998	0.648
40	0.998	0.649
50	0.998	0.649
100	0.998	0.649

To objectively demonstrate that the accuracy of our method is high even when different images databases are used and to avoid inconsistency in results with different image sets, the cover images were taken from the Uncompressed Color Image Database (UCID) image database [49]. The images in this database are color images. The color images were converted into grayscale images, and the same method was used to embed 1,000 images that were 512×512 pixels or 512×384 pixels in sizes for comparison. The results show that the proposed method in the various types of images detects suspicious images accurately and precisely (Tables 9, 10).

5 Discussion

The experimental results demonstrate that the proposed technique can clearly distinguish cover and stego images using a scatter diagram. In addition, the proposed technique is accurate and precise at low embedding ratios for various image sets and types of PVD interval classification tables. Although the WS steganalysis [40] is novel, the large number of false positive it produces renders it an unreliable steganalysis method. The WS steganalysis method [40] can estimate the embedding ratios in bits per pixel using the sum value. However, the partial parameters of the embedding process must be obtained, and the appropriate policy must be selected. By contrast, the proposed technique does not require the cover image to be obtained in advance.

Overall, the proposed method in the various types of images detects suspicious images accurately and precisely, even at low embedding ratios. In addition, our proposed method does not need to obtain the original image and embedding parameters, compared with the state-of-the-art method [40]. Therefore, our proposed method is a simpler and more effective technique compared with other steganalysis techniques.

6 Conclusions

In this study, we proposed a technique that addresses certain potential problems of the existing PVD steganography and steganalysis. We are motivated by the fact that relevant studies have focused on evading detection using RS analysis and PDH attack. However, RS analysis is aimed at the feature of the LSB substitution method, which is relatively less significant for PVD steganography. When the embedding ratio is low, the feature of the PDH is not clear. In addition, the state-of-the-art method [40] needs to obtain the original embedding parameters, which does not comply with a real detection situation. Therefore, we propose a simple and effective method based on statistical features for PVD steganalysis.

We conducted experiments with 1,000 images and found that our proposed method generally performed better than the other state-of-the-art methods across different image sets and embedding ratios. In terms of accuracy and precision, our method performs much better at low embedding ratios in the experiments. Therefore, our technique can serve as an effective tool for the steganalysis of PVD steganography and is a suitable alternative to the commonly used RS, PDH analysis, and WS steganography techniques. In particular, our method is expected to serve as a valuable addition to the toolkit of steganalysis techniques and digital forensics for the evaluation of PVD-based steganography in general and original PVD steganography techniques.

Abbreviations

PVD: Pixel-value differencing; LSB: Least significant bit; WS: Weighted stego image; RS: Regular-singular; PDH: Pixel difference histogram.

Acknowledgements

The authors would like to thank anonymous reviewers for their valuable comments and sharing their knowledge in improving this article.

Authors' contributions

THL conceptualized this study. KCC refined the idea. WBL performed the experiments and drafted the manuscript. All authors read and approved the final manuscript.

Funding

Not applicable.

Availability of data and materials

The datasets supporting the conclusions of this article are available in the BOSS (http://agents.fel.cvut.cz/stegodata/), BOWS2 (http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz), and UCID (https://qualinet.github.io/databases/image/uncompressed_colour_image_database_ucid/) repositories.

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1] School of Defense Science, Chung Cheng Institute of Technology, National Defense University, Taoyuan County, Taiwan, ROC. [2] Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan County, Taiwan, ROC. [3] Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan County, Taiwan, ROC.

Received: 19 May 2021 Accepted: 12 September 2021
Published online: 26 September 2021

References

1. W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding. IBM Syst. J. **35**(3.4), 313–336 (1996). https://doi.org/10.1147/sj.353.0313
2. J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color, and gray-scale images. IEEE Multimed. **8**(4), 22–28 (2001). https://doi.org/10.1109/93.959097
3. D.C. Wu, W.H. Tsai, A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett. **24**(9–10), 1613–1626 (2003). https://doi.org/10.1016/S0167-8655(02)00402-6
4. X. Zhang, S. Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett. **25**(3), 331–339 (2004). https://doi.org/10.1016/j.patrec.2003.10.014
5. H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proc. Vis. Image Signal Process. **152**(5), 611–615 (2005). https://doi.org/10.1049/ip-vis:20059022
6. C.H. Yang, C.Y. Weng, S.J. Wang, H.M. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Secur. **3**(3), 488–497 (2008). https://doi.org/10.1109/TIFS.2008.926097
7. C.H. Yang, C.Y. Weng, S.J. Wang, H.M. Sun, Varied PVD+LSB evading detection programs to spatial domain in data embedding systems. J. Syst. Softw. **83**(10), 1635–1643 (2010). https://doi.org/10.1016/j.jss.2010.03.081
8. X. Liao, Q. Wen, J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J. Vis. Commun. Image Represent. **22**(1), 1–8 (2011). https://doi.org/10.1016/j.jvcir.2010.08.007
9. K. Faez, M. Khodaei, New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image Process. **6**(6), 677–686 (2012). https://doi.org/10.1049/iet-ipr.2011.0059
10. M. Hussain, A.W.A. Wahab, N. Javed, K.H. Jung, Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Tech. Rev. **35**(1), 53–63 (2018). https://doi.org/10.1080/02564602.2016.1244496
11. K.H. Jung, Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. J. Real-Time Image Process. **14**(1), 127–136 (2018). https://doi.org/10.1007/s11554-017-0719-y
12. M.A. Hameed, M. Hassaballah, A. Aly, A.I. Awad, An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques. IEEE Access. **7**, 185189–185204 (2019). https://doi.org/10.1109/ACCESS.2019.2960254
13. M. Kalita, T. Tuithung, S. Majumder, An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. Cryptologia. **43**(5), 414–437 (2019). https://doi.org/10.1080/01611194.2019.1579122
14. H.H. Liu, P.C. Su, M.H. Hsu, An improved steganography method based on least-significant-bit substitution and pixel-value differencing. KSII Trans. Internet Inf. Syst. **14**(11), 4537–4556 (2020)
15. S. Singh, Adaptive PVD and LSB based high capacity data hiding scheme. Multimed. Tools Appl. **79**(25–26), 18815–18837 (2020). https://doi.org/10.1007/s11042-020-08745-5
16. H.H. Liu, Y.C. Lin, C.M. Lee, A digital data hiding scheme based on pixel-value differencing and side match method. Multimed. Tools Appl. **78**(9), 12157–12181 (2019). https://doi.org/10.1007/s11042-018-6766-y
17. S.Y. Shen, L.H. Huang, A data hiding scheme using pixel value differencing and improving exploiting modification directions. Comput. Secur. **48**, 131–141 (2015). https://doi.org/10.1016/j.cose.2014.07.008
18. S. Shen, L. Huang, S. Yu, A novel adaptive data hiding based on improved EMD and interpolation. Multimed. Tools Appl. **77**(10), 12563–12579 (2018). https://doi.org/10.1007/s11042-017-4905-5
19. K.C. Chang, C.P. Chang, P.S. Huang, T.M. Tu, A novel image steganographic method using tri-way pixel-value differencing. J. Multimed. **3**(2), 37–44 (2008). https://doi.org/10.4304/jmm.3.2.37-44
20. K.A. Darabkh, A new steganographic algorithm based on multi-directional PVD and modified LSB. Inf. Technol. Control **46**(1), 16–36 (2017). https://doi.org/10.5755/j01.itc.46.1.15253
21. A. Pradhan, K.R. Sekhar, G. Swain, Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks. Secur. Commun. Netw. **2017**, 1–13 (2017). https://doi.org/10.1155/2017/1924618
22. G. Swain, Digital image steganography using eight-directional PVD against RS analysis and PDH analysis. Adv. Multimed. **2018**, 1–13 (2018). https://doi.org/10.1155/2018/4847098
23. G. Swain, High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis. Secur. Commun. Netw. **2018**, 1–14 (2018). https://doi.org/10.1155/2018/1505896
24. M. Abdel Hameed, S. Aly, M. Hassaballah, An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). Multimed. Tools Appl. **77**(12), 14705–14723 (2018). https://doi.org/10.1007/s11042-017-5056-4
25. S. Kang, H. Park, J.I. Park, Combining LSB embedding with modified Octa-PVD embedding. Multimed. Tools Appl. **79**(29–30), 21155–21175 (2020). https://doi.org/10.1007/s11042-020-08925-3
26. C.M. Wang, N.I. Wu, C.S. Tsai, M.S. Hwang, A high quality steganographic method with pixel-value differencing and modulus function. J. Syst. Softw. **81**(1), 150–158 (2008). https://doi.org/10.1016/j.jss.2007.01.049
27. C.F. Lee, H.L. Chen, A novel data hiding scheme based on modulus function. J. Syst. Softw. **83**(5), 832–843 (2010). https://doi.org/10.1016/j.jss.2009.12.018
28. X. Liao, Q. Wen, J. Zhang, Improving the adaptive steganographic methods based on modulus function. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E96-A**(12), 2731–2734 (2013). https://doi.org/10.1587/transfun.E96.A.2731.
29. S. Shen, L. Huang, Q. Tian, A novel data hiding for color images based on pixel value difference and modulus function. Multimed. Tools Appl. **74**(3), 707–728 (2015). https://doi.org/10.1007/s11042-014-2016-0
30. W. Zhao, Z. Jie, L. Xin, W. Qiaoyan, Data embedding based on pixel value differencing and modulus function using indeterminate equation. J. China Univ. Posts Telecommun. **22**(1), 95–100 (2015). https://doi.org/10.1016/S1005-8885(15)60631-8
31. Z. Li, Y. He, Steganography with pixel-value differencing and modulus function based on PSO. J. Inf. Secur. Appl. **43**, 47–52 (2018). https://doi.org/10.1016/j.jisa.2018.10.006
32. A.K. Sahu, G. Swain, An optimal information hiding approach based on pixel value differencing and modulus function. Wirel. Pers. Commun. **108**(1), 159–174 (2019). https://doi.org/10.1007/s11277-019-06393-z
33. G. Swain, Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function. Optik **180**, 807–823 (2019). https://doi.org/10.1016/j.ijleo.2018.11.015

34. T.D. Sairam, K. Boopathybagan, An improved high capacity data hiding scheme using pixel value adjustment and modulus operation. Multimed. Tools Appl. **79**(23–24), 17003–17013 (2019). https://doi.org/10.1007/s11042-019-7557-9
35. J. Lu, G. Zhou, C. Yang, Z. Li, M. Lan, Steganalysis of content-adaptive steganography based on massive datasets pre-classification and feature selection. IEEE Access. **7**, 21702–21711 (2019). https://doi.org/10.1109/ACCESS.2019.2896781
36. D. Hu, S. Zhou, Q. Shen, S. Zheng, Z. Zhao, Y. Fan, Digital image steganalysis based on visual attention and deep reinforcement learning. IEEE Access. **7**, 25924–25935 (2019). https://doi.org/10.1109/ACCESS.2019.2900076
37. Z. Wang, M. Chen, Y. Yang, M. Lei, Z. Dong, Joint multi-domain feature learning for image steganalysis based on CNN. EURASIP J. Image Video Process. **2020**(1), 28 (2020). https://doi.org/10.1186/s13640-020-00513-7
38. T.S. Reinel, A.A.H. Brayan, B.O.M. Alejandro, M.R. Alejandro, A.G. Daniel, A.G.J. Alejandro, B.-J.A. Buenaventura, O.-A. Simon, I. Gustavo, R.P. Raul, GBRAS-Net: a convolutional neural network architecture for spatial image steganalysis. IEEE Access **9**, 14340–14350 (2021). https://doi.org/10.1109/ACCESS.2021.3052494
39. A.I. Iskanderani, I.M. Mehedi, A.J. Aljohani, M. Shorfuzzaman, F. Akther, T. Palaniswamy, S.A. Latif, A. Latif, Artificial intelligence-based digital image steganalysis. Secur. Commun. Networks. **2021**, 1–9 (2021). https://doi.org/10.1155/2021/9923389
40. H. Zhang, T. Zhang, H. Chen, Revisiting weighted stego-image steganalysis for PVD steganography. Multimed. Tools Appl. **78**(6), 7479–7497 (2019). https://doi.org/10.1007/s11042-018-6473-8
41. V. Sabeti, Sh. Samavi, M. Mahdavi, Sh. Shirani, Steganalysis of embedding in difference of image pixel pairs by neural network. ISC Int. J. Inf. Secur. (2009). https://doi.org/10.2204/isecure.2015.1.1.3
42. V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, Steganalysis and payload estimation of embedding in pixel differences using neural networks. Pattern Recognit. **43**(1), 405–415 (2010). https://doi.org/10.1016/j.patcog.2009.06.006
43. C.N. Bui, H.Y. Lee, J.C. Joo, H.K. Lee, Steganalysis method defeating the modified pixel-value differencing steganography. Int. J. Innov. Comput. Inf. Control **6**, 3193–3203 (2010)
44. N. Zaker, A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram. Multimed. Tools Appl. **58**(1), 147–166 (2012). https://doi.org/10.1007/s11042-010-0714-9
45. J.C. Joo, Histogram estimation-scheme-based steganalysis defeating the steganography using pixel-value differencing and modulus function. Opt. Eng. **49**(7), 077001 (2010). https://doi.org/10.1117/1.3463021
46. BOSS. Retrieved from http://agents.fel.cvut.cz/stegodata/. Accessed 15 July 2019.
47. K.Sayood, Introduction to Data Compression, Fifth (Katey Birtcher, 2006). https://doi.org/10.1016/C2015-0-06248-7.
48. BOWS2. Retrieved from http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz. Accessed 15 July 2019.
49. UCID. Retrieved from https://qualinet.github.io/databases/image/uncompressed_colour_image_database_ucid/. Accessed 22 Apr 2021.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com