Statistical Feature–Based Steganalysis for Pixel-Value Differencing Steganography

Wen-Bin Lin
   National Defense University Chung Cheng Institute of Technology

Tai-Hung Lai (✉ sudolai@gmail.com)
   National Chung Cheng University Library  https://orcid.org/0000-0002-0119-210X

Ko-Chin Chang
   National Defense University Chung Cheng Institute of Technology

Research

Keywords: Pixel-value differencing, Steganalysis, Steganography

Posted Date: May 24th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-512243/v1

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License
Statistical feature–based steganalysis for pixel-value differencing steganography

Wen-Bin Lin¹, Tai-Hung Lai²* and Ko-Chin Chang³

Abstract
The security and embedding capacity of pixel-value differencing (PVD) steganography is superior to that of least significant bit replacement steganography. Several studies have proposed extended PVD steganography methods that use the original concept of PVD steganography. The majority of the studies have verified their security against regular-singular detection analysis or pixel difference histogram attacks. Weighted stego image steganalysis is the state-of-the-art technology for PVD steganography. This study proposed a suitable parameter for the estimator based on different relative embedding ratios and the size of normal embedding blocks. The experimental results revealed that the proposed technology does not require advance knowledge of the original image. In addition, the proposed method is accurate and precise at any embedding ratio. In the future, this method may be utilized to analyze the security of extended PVD steganography.

Keywords: Pixel-value differencing, Steganalysis, Steganography

1 Introduction
Cryptography and data hiding are used to protect secure information. Encryption keys convert secret data into unrecognizable random numbers to prevent illegal obtainment. Long-encrypted keys can ensure data security, but the random numbers generated after encryption are likely to draw the attention of criminals. Data-hiding technology can conceal data in carriers without changing the original data. Common carriers include video, audio, text, and images. Compared with other carriers, digital images have considerable redundant space. For this reason, digital images are commonly used for steganography and are called “cover images”; images with embedded information are called “stego images.” Steganography techniques can be categorized as compression domain, frequency domain, and spatial domain.

In spatial domain techniques, pixel values are changed directly; for example, in least significant bit replacement (LSBR) steganography, secret data are embedded by flipping the least significant bit (LSB) of the pixel value [1]. However, the LSBR algorithm can be detected through regular-singular (RS) analysis attacks. The pixel-value differencing (PVD) method [2] was developed to resist RS detection and improve embedding capacity. Zhang et al. proposed a modified method that improved the PVD algorithm by incorporating the detection of step-like features on PVD histograms [3]. The concept of PVD has been applied to steganography in PVD steganography. The integration of PVD with LSBR steganography involves using the concept of PVD to distinguish smooth and complex textures in an image and replacing LSBs with three pixel values to increase embedding capacity [4–14]. Modulus-based PVD steganography uses the concept of congruence in modular arithmetic to hide secret information [15–23]. In the side-match scheme [24], steganography is integrated with PVD and the side-match method is used to embed secret information in pixels of an embedded block, thereby increasing embedding capacity. The multidirectional PVD method uses the differences between pixels in different directions in secret blocks to hide information and increase the amount of hidden information [25–31]. Studies have proposed steganalysis methods based on machine learning and deep learning methods [32,33], but these techniques require considerable computing resources. In a statistical characteristic–based steganalysis, Joo et al. [34] used the changes in a pixel difference histogram (PDH) to detect modulus PVD steganography. Zaker et al. [35] also used PDH to detect tri-way PVD, and Zhang et al. [36] proposed PVD noise steganalysis with weighted stego image (WS) estimators.

PVD-related steganography techniques prioritize increasing embedding capacity and maintaining image quality, but the validation of security is oriented toward defeating RS analysis and PDH attacks. Therefore, we proposed a statistical feature–based

* Correspondence: sudolai@gmail.com

²Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan, Taiwan
method for PVD steganography. Compared with state-of-the-art steganalysis, the proposed method is more accurate and precise at every embedding ratio and can be performed without obtaining the original cover image.

This article is organized as follows: Section 2 describes several related techniques; Section 3 details the proposed method for PVD steganography; Section 4 presents the experimental results and discussion; and Section 5 concludes the article.

2 Related works

2.1 PVD steganography

PVD steganography was proposed by Wu et al. [2]. This method is based on small variations that are discerned more easily by human vision in smooth areas than in edge areas. PVD can be utilized to distinguish smooth areas and edge areas. A small amount of secret information is embedded in smooth areas and a large amount of data is embedded in edge areas. Tables 1 and 2 present the steganographic parameters required to implement this method. First, an image is divided in a zigzag manner into sections of two adjacent and nonoverlapping pixels. The differences in the pairs of pixels are calculated to obtain the number of embedding bits, as displayed in Tables 1 and 2.

The pixel values are assumed to be \( p_i \) and \( p_{i+1} \). The absolute value of difference \( d \) is divided into consecutive ranges. The lower bound of the range interval is defined as \( l_i \). Tables 1 and 2 present the parameters of the range intervals for the various differences in pixel values. Binary secret bits are converted into decimal value \( b \), and the new difference is calculated as follows:

\[
d' = \begin{cases} 
  l_i + b, & \text{if } d \geq 0 \\
  -(l_i + b), & \text{if } d < 0 
\end{cases}
\]  

(1)

If stego image pixels with values of \( p_i \) and \( p_{i+1} \) have difference \( d' \), then the embedding process is as follows:

\[
\begin{cases} 
  (p_i - \left\lfloor \frac{d' - d}{2} \right\rfloor, p_{i+1} + \left\lfloor \frac{d' - d}{2} \right\rfloor), & \text{if } d \text{ is odd} \\
  (g_i - \left\lfloor \frac{d' - d}{2} \right\rfloor, g_{i+1} + \left\lfloor \frac{d' - d}{2} \right\rfloor), & \text{if } d \text{ is even}
\end{cases}
\]  

(2)

These definitions serve as the basis for the steganalysis detection technique detailed in the subsequent section.

### Table 1 Type 1 range table

| Interval \((k)\) | 1  | 2  | 3  | 4  | 5  | 6  |
|-----------------|----|----|----|----|----|----|
| Range \((R_k)\) | [0,7] | [8,15] | [16,31] | [32,63] | [64,127] | [128,255] |
| Lower limit \((l_k)\) | 0 | 8 | 16 | 32 | 64 | 128 |
| Upper limit \((u_k)\) | 7 | 15 | 31 | 63 | 127 | 255 |
| Range width \((w_k)\) | 8 | 8 | 16 | 32 | 64 | 128 |
| Capacity \((n)\) | 3 | 3 | 4 | 5 | 6 | 7 |

### Table 2 Type 2 range table

| Interval \((k)\) | Range \((R_k)\) | Lower limit \((l_k)\) | Upper limit \((u_k)\) | Range width \((w_k)\) | Capacity \((n)\) |
|-----------------|----------------|----------------|----------------|----------------|---------|
| 1 | [0,1] | 0 | 1 | 2 | 1 |
| 2 | [2,3] | 2 | 3 | 2 | 1 |
| 3 | [4,7] | 4 | 7 | 4 | 2 |
| 4 | [8,11] | 8 | 11 | 4 | 2 |
| 5 | [12,15] | 12 | 15 | 4 | 2 |
| 6 | [16,23] | 16 | 23 | 8 | 3 |
| 7 | [24,31] | 24 | 31 | 8 | 3 |
2.2 WS steganalysis
Zhang et al. [36] proposed a WS steganalysis method for PVD steganography. In this method, the feature of the stego noise in sum value images is similar to that of LSBR steganography. This method only involves normal embedding blocks, which are denoted by $A$. The maximal embedding ratio in bits per pixel is as follows:

$$r_{\text{max}} = \frac{|A|}{2N} \sum_{i \in A} P(|d_i| \in R_k \mid i \in A) \log_2(w_i),$$

(3)

where $N$ is the number of pixel pairs.

The estimator of a cover image is denoted as $\hat{c}$, and it is obtained by using local linear predictor with fixed forms as shown in (4).

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

(4)

Then, the residuals are calculated as follows:

$$r_i = (s_i - \hat{s}_i) \ast (s_i - \hat{c}),$$

(5)

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

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

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

(6)

where $\lambda$ is a constant ($\lambda = 5$).

WS residuals in the sum value of the stego image are calculated, and an LSBR embedding rate is estimated by using (7).

$$\hat{p} = \frac{2 \sum_{i \in A} w(\sigma_i)r_i}{\sum_{i \in A} w(\sigma_i)}$$

(7)

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

$$\hat{r} = r_{\text{max}} \ast \hat{p} = \frac{2r_{\text{max}} \sum_{i \in A} w(\sigma_i)r_i}{\sum_{i \in A} w(\sigma_i)}$$

(8)

If $\hat{r} < 0$, $\hat{r}$ must be corrected to be zero. However, if $\hat{r} > r_{\text{max}}$, $\hat{r}$ must be corrected to be $r_{\text{max}}$. This method indicates that estimators are sensitive to sample size and relative embedding rate.

3 Proposed method
In this section, we describe our method for PVD steganalysis. This method involves two phases: the first phase is the analysis of PVD steganography, and the second phase is the detection of steganography. The drawbacks of PVD steganography are analyzed in Section 3.1. A method of detection based on these drawbacks is proposed in Section 3.2. Pre-embedding images are referred to as “cover images,” and embedding images are referred to as “stego images.” Differences between pixel pairs are denoted as $d$. The frequencies of a difference $d$ in the cover and stego images are defined as $h(d)$ and $h'(d)$, respectively; the bin range in the histogram is $-32$ to $32$. 
3.1 Analyses of PVD steganography

Fig. 1 presents the analytical process of the proposed method. In this study, secret binary bitstreams were randomly generated using a uniform distribution. Grayscale image sets from the Break Our Steganographic System (BOSS) database were used, and we assumed that the cover images were compressed. Therefore, the frequency of the smooth areas was higher than that of the complex areas in the texture of a test image. The histogram of pixel-value difference exhibited a Laplace distribution.

First, the characteristics of pixel-value difference in a cover image and a stego image were analyzed. The type 1 difference range interval was used to embed secret bitstreams. Secret bitstreams were embedded at an embedding ratio of 100% to generate a stego image. Figs. 2 and 3 present the PDHs of the cover and stego images, respectively. Fig. 2 indicates a Laplace distribution symmetrical between \( h(1) \) and \( h(-1) \). The histogram in Fig. 3 is asymmetrical and has a step-like shape in the bin range of \(-7 \) to \( 7 \). Secret bitstreams were embedded at an embedding ratio of 10%. In Fig. 4, the histogram is slightly asymmetrical in the bin range of \(-7 \) to \( 7 \).

Second, the type 2 difference range interval was used to embed secret bitstreams at an embedding ratio of 100%. Figs. 5 and 6 display the PDHs of the cover and stego images, respectively. Fig. 5 indicates that the histogram has a step-like shape and is slightly asymmetrical in the bin range of \(-7 \) to \( 7 \). Secret bitstreams were embedded at an embedding ratio of 10%. In Fig. 6, the histogram is slightly asymmetrical in the bin range of \(-7 \) to \( 7 \).

Fig. 1 Block diagram of the analytic process
Fig. 2 Histogram of pixel-value difference

Fig. 3 Histogram of PVD steganography using type 1 range interval at an embedding ratio of 100%
Fig. 4 Histogram of PVD steganography using type 1 range interval at an embedding ratio of 10%.

Fig. 5 Histogram of PVD steganography using type 2 range interval at an embedding ratio of 100%.
3.2 Steganalysis of PVD technique

In practice, suspicious images are indeterminate. The proposed method is based on the symmetry of Laplacian distributions. Although the original images may be unavailable, the steganography function only changes the LSB. Therefore, the sum of the two frequencies does not change. The theoretically expected frequency can be obtained from any random test image without obtaining the cover image. We assumed the test image was a cover image and compared the theoretically expected frequency with the observed frequency. The expected frequency is the mean of the frequencies of pixel pair differences. The proposed method involves focusing on the degree of similarity between the expected and observed frequencies. We obtained the difference between the theoretically expected frequency and the observed frequency in the detection process. Let $H_i$ and $E(H_i)$ denote the set of detecting pairs and the expected value of $H_i$, respectively, as shown in (9).

$$H_i = \{ h(-d_i), h(d_i) \}$$

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

The proposed method uses seven $H$ values to calculate the function of the feature as follows:

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

where $n$ is the number of $H_i$ values.

If a test image is a cover image, the theoretically expected value is approximately the same as the observed value. The value of the feature should be as small as possible, and the value of the feature of a stego image should be high. We selected an appropriate threshold to distinguish a cover image from a stego image. For a cover image, the value of the feature is less than the threshold, and for a stego image, the value of the feature is higher than the threshold.
4 Experimental results and discussion

This section describes the extensive experiments conducted to validate the proposed method. The experimental environment was implemented by using MATLAB R2018a (MathWorks, Natick, MA, USA) on an Intel Core i5-8250U with 8 GB of RAM. We used validation sets from the BOSS [37], Break Our Watermarking System 2 (BOWS2) [38], and Uncompressed Color Image Database (UCID) [39] image databases. The BOSS and BOWS2 image databases contain grayscale images with dimensions of 512 × 512 pixels. The UCID image database consists of color images with dimensions of 384 × 512 pixels or 512 × 384 pixels. We randomly selected 1,000 images as the test sets for our experiments. Secret bitstreams were simulated with the MATLAB random number generator, and a threshold value of 1 was obtained from the experiments. We considered the detection of steganalysis as the binary classification problem with which to measure the effectiveness of the proposed method. Prediction of whether the suspicious image is a stego image or a cover image is divided into the four following 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 detection performance. The accuracy metric refers to the proportion of correctly predicted classes. The precision metric refers to the proportion of positive predictions that are correct. Both accuracy and precision should be as high as possible. Accuracy and precision are calculated by using (11) and (12), respectively.
4.1 Analysis of experimental results

The experimental analysis was divided into two processes on the basis of the difference range interval of the pixel pair (i.e., type 1 or type 2). For the first experiment, we analyzed the type 1 difference range interval. We randomly selected 1,000 images from the 10,000 images in the BOSS image set as the cover images and used embedding ratios of 10% and 100% to generate 1,000 stego images. The proposed technique was used to obtain the feature values of the cover and stego images. We created diagrams for the distribution of the 1,000 stego images at embedding ratios of 10% and 100% (Figs. 8 and 9, respectively). A comparison of the distributions of the cover and stego images at embedding ratios of 10% and 100% indicated that the cover and stego images were clearly distinguished through this method.

The distribution of the cover and stego images indicated that when the suspicious image is a cover image, the value of the feature is low. When the suspicious image is a stego image, the value of the feature is higher. A suitable threshold value (1) for \( F \) was obtained through experimentation.

![Fig. 8](image)

**Fig. 8** Distribution of cover and stego images at an embedding ratio of 100% for type 1
The experiment based on the type 2 difference range interval was evaluated by using the same method, and diagrams for the distributions of the 1,000 stego images at embedding ratios of 10% and 100% were prepared (Figs. 10 and 11, respectively). A comparison of the distributions of the cover and stego images at embedding ratios of 10% and 100% indicated that the cover and stego images were clearly distinguished through this method. The threshold value (1) was the same.

Fig. 9 Distribution of cover and stego images at an embedding ratio of 10% for type 1

Fig. 10 Distribution of cover and stego images with an embedding ratio of 100% for type 2
Table 3 indicates that the accuracy of the proposed method under a threshold value of 1 for type 1 was greater than 90% at any embedding ratio. Table 4 indicates that the accuracy of the proposed method under a threshold value of 1 for type 2 was also greater than 90%, even at any embedding ratios.

**Table 3** Results of the proposed technique for type 1

| Embedding ratio (%) | TP   | FN   | TN   | FP   | Accuracy |
|---------------------|------|------|------|------|----------|
| 10                  | 942  | 58   | 930  | 70   | 0.936    |
| 20                  | 984  | 16   | 930  | 70   | 0.957    |
| 30                  | 1000 | 0    | 930  | 70   | 0.965    |
| 40                  | 1000 | 0    | 930  | 70   | 0.965    |
| 50                  | 1000 | 0    | 930  | 70   | 0.965    |
| 60                  | 1000 | 0    | 930  | 70   | 0.965    |
| 70                  | 1000 | 0    | 930  | 70   | 0.965    |
| 80                  | 1000 | 0    | 930  | 70   | 0.965    |
| 90                  | 1000 | 0    | 930  | 70   | 0.965    |
| 100                 | 1000 | 0    | 930  | 70   | 0.965    |

**Table 4** Results of the proposed technique for type 2

| Embedding ratio (%) | TP   | FN   | TN   | FP   | Accuracy |
|---------------------|------|------|------|------|----------|
| 10                  | 937  | 63   | 972  | 28   | 0.955    |
| 20                  | 990  | 10   | 972  | 28   | 0.981    |
| 30                  | 997  | 3    | 972  | 28   | 0.985    |
| 40                  | 998  | 2    | 972  | 28   | 0.985    |
| 50                  | 998  | 2    | 972  | 28   | 0.985    |
4.2 Comparative analysis with state-of-the-art techniques

To prove the superiority of the proposed steganalysis technique, we compared this technique with other methods by using various types of images and embedding ratios. Zhang et al. [36] indicated the best option for the WS estimator. The majority of the parameters for the estimator were within the relative embedding ratio, and the size of the concealable area was small. The local linear predictor with fixed model $T$ exhibited the best estimation performance. The estimator value of a cover image should be zero. Therefore, we assumed the threshold to be zero. We randomly selected 1,000 images from the 10,000 images in the BOSS [37] and BOWS2 [38] image databases. The common type 1 model proposed by Wu et al. [2] was adopted to generate 1,000 stego images from each image database with embedding ratios of 10%, 20%, 30%, 40%, 50%, and 100%. We then evaluated the accuracy and precision of our technique with that of the technique in the work of Zhang et al. [36] (Tables 5, 6, 7, and 8, respectively). The results revealed that the proposed method detects suspicious images accurately and precisely with a low rate of misjudgment.

| Table 5 | Comparison of accuracy of methods for BOSS image database |
|---------|----------------------------------------------------------|
| Embedding ratio (%) | Proposed method | Zhang et al.’s method [36] |
| 10      | 0.936          | 0.742 |
| 20      | 0.957          | 0.751 |
| 30      | 0.965          | 0.757 |
| 40      | 0.965          | 0.757 |
| 50      | 0.965          | 0.756 |
| 100     | 0.965          | 0.757 |

| Table 6 | Comparison of precision of methods for BOSS image database |
|---------|------------------------------------------------------------|
| Embedding ratio (%) | Proposed method | Zhang et al.’s method [36] |
| 10      | 0.931           | 0.666 |
| 20      | 0.934           | 0.671 |
| 30      | 0.935           | 0.673 |
| 40      | 0.935           | 0.673 |
| 50      | 0.935           | 0.673 |
| 100     | 0.935           | 0.673 |

| Table 7 | Comparison of accuracy of methods for BOWS2 image database |
|---------|-----------------------------------------------------------|
| Embedding ratio (%) | Proposed method | Zhang et al.’s method [36] |
| 10      | 0.948           | 0.758 |
| 20      | 0.980           | 0.769 |
| 30      | 0.987           | 0.769 |
| 40      | 0.987           | 0.770 |
| 50      | 0.988           | 0.770 |
Table 8 Comparison of precision of methods for BOWS2 database image

| Embedding ratio (%) | Proposed method | Zhang et al.’s method[36] |
|---------------------|-----------------|--------------------------|
| 10                  | 0.974           | 0.680                    |
| 20                  | 0.975           | 0.685                    |
| 30                  | 0.976           | 0.685                    |
| 40                  | 0.976           | 0.686                    |
| 50                  | 0.976           | 0.686                    |
| 100                 | 0.976           | 0.686                    |

To demonstrate that the experimental results of the proposed technique were consistent for each image database, we randomly selected 1,000 color images from the set of 1,388 color images in the UCID database for validation. The test images were first converted to grayscale and then verified by using the same method. Tables 9 and 10 compare the accuracy and precision of the methods.

Table 9 Comparison of accuracy for UCID database images

| Embedding ratio (%) | Proposed method | Zhang et al.’s method[36] |
|---------------------|-----------------|--------------------------|
| 10                  | 0.925           | 0.716                    |
| 20                  | 0.972           | 0.725                    |
| 30                  | 0.983           | 0.728                    |
| 40                  | 0.983           | 0.730                    |
| 50                  | 0.983           | 0.729                    |
| 100                 | 0.983           | 0.730                    |

Table 10 Comparison of precision for UCID database images

| Embedding ratio (%) | Proposed method | Zhang et al.’s method[36] |
|---------------------|-----------------|--------------------------|
| 10                  | 0.963           | 0.643                    |
| 20                  | 0.966           | 0.647                    |
| 30                  | 0.967           | 0.648                    |
| 40                  | 0.967           | 0.649                    |
| 50                  | 0.967           | 0.649                    |
| 100                 | 0.967           | 0.649                    |

4.3 Discussion

The experimental results demonstrated that the proposed technique can clearly distinguish cover and stego images by using a scatter diagram. In addition, the proposed technique is accurate and precise at any embedding ratio for various image sets and range interval types. Although the state-of-the-art WS steganalysis method for PVD steganography [36] is novel, the large number of false positive it produces renders it unreliable method of steganalysis. The WS steganalysis method can estimate the embedding ratio in bits per pixel by using sum value. However, the partial parameters of the cover 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.

5 Conclusion

This study proposed a statistical feature–based steganalysis method for PVD steganography. Although
several studies have been conducted on PVD ste- 
ganography, few have investigated PVD steganalysis 
methods. Studies on PVD steganography have gen-
erally concluded that it is a safe option and can effec-
tively avoid RS detection analysis and PDH attacks. 
The experimental results of this study indicated that 
the proposed technique can effectively detect PVD 
steoganography for various types of images at any 
embedding ratio. In addition, the proposed method 
does not require knowledge of the cover image in 
advance, and in a comparison with another 
state-of-the-art technology, the proposed misjudged 
fewer images. The results suggest that the proposed 
technique is a reliable method of steganalysis and can 
effectively detect the security features of PVD ste-
ganography.

**Abbreviations**
PVD: pixel-value differencing; LSB: least significant 
bit; LSBR: least significant bit replacement; WS: 
weighted stego image; RS: regular-singular; PDH: 
pixel difference histogram.

**Acknowledgments**
This manuscript was edited by Wallace Academic 
Editing.

**Authors’ contributions**
TL conceptualized this study. KC refined the idea. 
WL performed the experiments and drafted the manu-
script. All authors read and approved the manu-
script.

**Authors’ information**
Tai-Hung Lai is currently an Assistant Professor in 
the Department of Computer Science and Informa-
tion Engineering at National Defense University, 
Taiwan. His research interests include digital image 
steoganography and network security.
Ko-Chin Chang is currently an Associate Professor 
in the Department of Computer Science and Informa-
tion Engineering, Chung Cheng Institute of Technology, National Defense University, 
Taiwan. His research interests include network security and digi-
tal forensics.
Wen-Bin Li is currently working toward a PhD at the 
Chung Cheng Institute of Technology, National De-
fense University. His research interests include im-
age steoganography and steganalysis.

**Funding**
Not applicable.

**Availability of data and materials**
The datasets supporting the conclusions of this article 
are available in the BOSS 
(http://www.agents.cz/boss/BOSSFinal/index.php?m 
de=VIEW&tmpl=materials), BOWS2 
(http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz), and 
UCID 
(https://qualinet.github.io/databases/image/uncompre 
sed_colour_image_database_ucid/) repositories.

**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, 
Taiyuan County, Taiwan. 2 Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University, 
Taiyuan County, Taiwan. 3 Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University, 
Taiyuan County, Taiwan.

**References**
1. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, 
Techniques for data hiding. IBM Syst. J. 35, 
313–336 (1996).
2. D.-C. Wu and W.-H. Tsai, A steganographic 
method for images by pixel-value differencing. 
Pattern Recognition Letters 24, 1613–1626 
(2003).
3. X. Zhang and S. Wang, Vulnerability of pix-
el-value differencing steganography to histo-
gram analysis and modification for enhanced 
security. Pattern Recognition Letters 25, 
331–339 (2004).
4. H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. 
Hwang. Image steganographic scheme based on 
pixel-value differencing and LSB replacement 
methods. IEE Proceedings - Vision, Image and 
Signal Processing 152, 611–615 (2005).
5. C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. 
Sun. Varied PVD+LSB evading detection pro-
grams to spatial domain in data embedding sys-
tems. Journal of Systems and Software 83, 
1635–1643 (2010).
6. K. Faiez and M. Khodaei, New adaptive ste-
ganographic method using least-significant-bit
substitution and pixel-value differencing. IET Image Processing 6, 677–686 (2012).
7. X. Liao, Q. Wen, and J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution. Journal of Visual Communication and Image Representation 22, 1–8 (2011).
8. C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems. IEEE Trans.Inform.Forensic Secur. 3, 488–497 (2008).
9. M. Hussain, A. W. A. Wahab, N. Javed, and K.-H. Jung, Recursive Information Hiding Scheme Through LSB, PVD Shift, and MPE. IETE Technical Review 35, 53–63 (2018).
10. K.-H. Jung, Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. J Real-Time Image Proc 14, 127–136 (2018).
11. M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques. IEEE Access 7, 185189–185204 (2019).
12. M. Kalita, T. Tuithung, and S. Majumder, An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. Cryptologia 43, 414–437 (2019).
13. H.-H. Liu, P.-C. Su, and M.-H. Hsu, An Improved Steganography Method Based on Least-Significant-Bit Substitution and Pixel-Value Differencing. KSII Transactions on Internet and Information Systems 14, 4537–4556 (2020).
14. S. Singh, Adaptive PVD and LSB based high capacity data hiding scheme. Multimed Tools Appl 79, 18815–18837 (2020).
15. C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, A high quality steganographic method with pixel-value differencing and modulus function. Journal of Systems and Software 81, 150–158 (2008).
16. C.-F. Lee and H.-L. Chen, A novel data hiding scheme based on modulus function. Journal of Systems and Software 83, 832–843 (2010).
17. T. D. Sairam and K. Boopathybagan, An improved high capacity data hiding scheme using pixel value adjustment and modulus operation. Multimed Tools Appl 79, 17003–17013 (2020).
18. S. Shen, L. Huang, and Q. Tian, A novel data hiding for color images based on pixel value difference and modulus function. Multimed Tools Appl 74, 707–728 (2015).
19. W. Zhao, Z. Jie, L. Xin, and W. Qiao, Data embedding based on pixel value differencing and modulus function using indeterminate equation. The Journal of China Universities of Posts and Telecommunications 22, 95–100 (2015).
20. Z. Li and Y. He, Steganography with pixel-value differencing and modulus function based on PSO. Journal of Information Security and Applications 43, 47–52 (2018).
21. A. K. Sahu and G. Swain, An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function. Wireless Pers Commun 108, 159–174 (2019).
22. 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).
23. X. Liao, Q. Wen, and J. Zhang, Improving the Adaptive Steganographic Methods Based on Modulus Function. IEICE Trans. Fundamentals E96.A, 2731–2734 (2013).
24. H.-H. Liu, Y.-C. Lin, and C.-M. Lee, A digital data hiding scheme based on pixel-value differencing and side match method. Multimed Tools Appl 78, 12157–12181 (2019).
25. K. A. Darabkh, A New Steganographic Algorithm Based on Multi Directional PVD and Modified LSB. ITC 46, 16–36 (2017).
26. A. Pradhan, K. R. Sekhar, and G. Swain, Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks. Security and Communication Networks 2017, 1–13 (2017).
27. G. Swain, Digital Image Steganography Using Eight-Directional PVD against RS Analysis and PDH Analysis. Advances in Multimedia 2018, 1–13 (2018).
28. G. Swain, High Capacity Image Steganography Using Modified LSB Substitution and PVD against Pixel Difference Histogram Analysis. Security and Communication Networks 2018, 1–14 (2018).
29. M. Abdel Hameed, S. Aly, and M. Hassaballah, An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). Multimed Tools Appl 77, 14705–14723 (2018).
30. P.-H. Kim, E.-J. Yoon, K.-W. Ryu, and K.-H. Jung, Data-Hiding Scheme Using Multidirectional Pixel-Value Differencing on Colour Images. Security and Communication Networks 2019, 1–11 (2019).
31. S. Kang, H. Park, and J.-I. Park, Combining LSB embedding with modified Octa-PVD embedding. Multimed Tools Appl 79, 21155–21175 (2020).
32. Z. Wang, M. Chen, Y. Yang, M. Lei, and Z. Dong, Joint multi-domain feature learning for image steganalysis based on CNN. J Image Video Proc. 2020, 28 (2020).
33. M. Dalal and M. Juneja, Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimed Tools Appl 80, 5723–5771 (2021).
34. J.-C. Joo, Histogram estimation-scheme-based steganalysis defeating the steganography using pixel-value differencing and modulus function. Opt. Eng 49, 077001 (2010).
35. N. Zaker and A. Hamzeh, A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram. Multimed Tools Appl 58, 147–166 (2012).
36. H. Zhang, T. Zhang, and H. Chen, Revisiting weighted Stego-image Steganalysis for PVD steganography. Multimed Tools Appl 78, 7479–7497 (2019).
37. http://www.agents.cz/boss/BOSSFinal/index.php?mode=VIEW&tmpl=materials
38. http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz
39. https://qualinet.github.io/databases/image/uncompressed_colour_image_database_ucid/
Figure 1

Block diagram of the analytic process
Figure 2

Histogram of pixel-value difference
Figure 3

Histogram of PVD steganography using type 1 range interval at an embedding ratio of 100%
Figure 4

Histogram of PVD steganography using type 1 range interval at an embedding ratio of 10%
Figure 5

Histogram of PVD steganography using type 2 range interval at an embedding ratio of 100%
Figure 6

Histogram of PVD steganography using type 2 range interval at an embedding ratio of 10%
Figure 7

Flow chart of the proposed technique
Figure 8

Distribution of cover and stego images at an embedding ratio of 100% for type 1
Figure 9

Distribution of cover and stego images at an embedding ratio of 10% for type 1
Figure 10

Distribution of cover and stego images with an embedding ratio of 100% for type 2
Figure 11

Distribution of cover and stego images with an embedding ratio of 10% for type 2