International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **11**, November **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 6571–6583

STEGANALYSIS OF HISTOGRAM MODIFICATION REVERSIBLE DATA HIDING SCHEME BY HISTOGRAM FEATURE CODING

Der-Chyuan Lou[1], Chen-Hao Hu[2] and Chung-Cheng Chiu[2]

[1]Department of Computer Science and Information Engineering
Chang Gung University
No. 259, Wen-Hwa 1st Rd., Kwei-Shan, Taoyuan 333, Taiwan
dclouprof@gmail.com

[2]Department of Electrical and Electronic Engineering
Chung Cheng Institute of Technology
National Defense University
No. 190, Sanyuan 1st St., Dashi Jen, Taoyuan 335, Taiwan
chenhao.hu@gmail.com; davidchiu@ndu.edu.tw

Received July 2010; revised November 2010

Abstract. *In 2006, Ni et al. proposed a reversible data-hiding algorithm based on histogram modification that utilizes the zero points and maximum points of the histogram of an image to slightly modify the pixel grayscale values to embed messages into an image. Reversible data-hiding schemes assure that the original cover image can be completely recovered from the stego-image after the hidden messages are extracted. Such data-hiding techniques are suitable for applications in the military, medicine, high-energy particle physical experimental investigation and art in cases in which any distortion to the original images is not acceptable. Steganalysis techniques are used to identify possibly hidden images from cover images or determine whether there are messages embedded in cover images. In this paper, a novel steganalytic scheme that can detect the present of Ni et al.'s steganographic method and that is based on histogram feature coding is proposed. Experimental results show that the steganalytic scheme is capable of detecting Ni et al.'s steganographic method.*

Keywords: Data hiding, Information hiding, Digital watermarking, Steganalysis, Reversible data hiding

1. **Introduction.** Data hiding [1-3] is a process to hide secret messages in a cover media to make them undetectable. The main goal of data hiding is to enhance communication security by embedding secret messages into an inconspicuous carrier and thereby transmit them to the receiver. Hence, embedding capacity and imperceptibility are two important dimensions of data-hiding methods. However, at present, another important, broadly researched issue is the reversibility of data hiding. In general, the embedding process involved in data hiding overrides the original data of the selected carrier, which cannot be restored at the receiver side. Reversible data-hiding techniques aim to solve these problems. Reversible data-hiding techniques [4-7] not only can hide the secret messages in a cover carrier, but also can provide a lossless reconstruction of the original cover carrier after the secret messages are extracted. Reversible data-hiding techniques satisfy some applications that demand no distortion, such as in the military, medicine, high-energy particle physical experimental investigation and art.

In contrast to data hiding, the goal of steganalysis is to detect the presence of secret messages or determine a steganographic method. Current steganalysis techniques [8] fall broadly into one of two categories: specific [9,10] or universal blind steganalysis [11-13]. Specific steganalysis can examine the presence of a secret message embedded by a specific steganographic algorithm or perhaps estimate the embedding ratio. Universal blind steganalysis is a meta-detection method in the sense it can be adjusted to detect most well known steganographic methods after training on a substantial amount of original and stego-media. In general, steganalysis methods that target a specific embedding method can provide more accurate and reliable results than any other universal blind steganalysis.

In 2006, Ni et al. proposed a reversible data-hiding algorithm based on histogram modification [7] with low computational complexity and short execution time. Thus far, no steganalytic method proposed has been effectual against it. In 2008, Kuo and Lin [14] introduced a steganalysis method to attack histogram modification-based reversible data hiding schemes using relationship analysis of five continuous pixel pairs in an image histogram. However, their method only works on cover images with smooth histogram distributions. Therefore, their steganalysis method can only detect the stego-images generated from cover images with a smooth histogram distribution. However, we found that there are many different histogram distributions among a sample of downloaded images on the Internet, some of which would make the stego-images resistant to the Kuo and Lin's steganalysis method. In this paper, we investigate the overall differences in histogram features between cover images and stego-images and propose a novel specific steganalysis method to detect the presence of the stego-images implemented with Ni et al.'s reversible data-hiding algorithm in many types of images. In addition, we introduced a histogram coding method to reduce the computation complexity of steganalysis. Through the proposed sampling and quantifying processes, image histogram feature codes are encoded. By depending on these histogram feature codes, the stego-images can be detected efficiently.

2. Review of the Ni et al.'s Reversible Data-Hiding Method.

In 2006, Ni et al.'s reversible data-hiding scheme used peak points in an image to hide messages based on histogram modification. The scheme can embed a large amount (5-80 Kb for a 512×512×8 bits grayscale image) of data while maintaining a very high visual quality for all natural images. The Peak signal-to-noise ratio (PSNR) of the stego-image, compared with the original image, is guaranteed to be higher than 48dB [7]. The hiding capacity is associated with the pixel number of the peak points in a cover image. Therefore, as the pixel number of the peak points increases, the hiding capacity also increases. Ni et al.'s reversible data-hiding scheme is implemented as follows.

2.1. Embedding phase.

Step 1: Choose k pairs of reversible keys consisting of the maximum points $Max(a_i)$ and the minimum points $Min(b_i)$ of a cover image histogram, where $i = 1, 2, \ldots, k$. Address each pair one-by-one using the following steps.

Step 2: The maximum points $Max(a_i)$ are the peak points, and the minimum points $Min(b_i)$ are the zero points. If the number of these zero points is not equal to zero, record the pixel positions of these zero points as overhead book-keeping information. This is used to recover those pixels in data-extracting and data-restoring steps in order to recover the original cover image.

Step 3: Denote the pixel value x of a pixel of the cover image I within the range from $Max(a_i)$ to $Min(b_i)$ as $x \in (Max(a_i), Min(b_i))$. Then, the pixel value x can be replaced by Equation (1).

$$\begin{cases} x = x + 1 & \text{if } Max(a_i) < Min(b_i); \\ x = x - 1 & \text{if } Max(a_i) > Min(b_i). \end{cases} \tag{1}$$

Step 4: Scan the cover image in a specific order and embed data m (i.e., messages and overhead) into the pixels with a pixel value of $Max(a_i)$ using Equation (2).

$$\begin{cases} Max(a_i) = Max(a_i) + 1 & \text{if } m = 1 \text{ and } Max(a_i) < Max(b_i); \\ Max(a_i) = Max(a_i) - 1 & \text{if } m = 1 \text{ and } Max(a_i) > Max(b_i); \\ \text{Otherwise keep } Max(a_i) \text{ unchanged.} \end{cases} \tag{2}$$

2.2. The extracting and restoring phase.

Step 1: Scan the marked image in the same sequential order as in the embedding phase. When the pixel value is equal to $(Max(a_i) + 1)$, message bit "1" is extracted; when the pixel value is equal to $Max(a_i)$, message bit "0" is extracted.

Step 2: Reset the pixel values of the peak points that were changed in the embedding phase. If the pixel value of a pixel x is equal to $Max(a) + 1$, then set the pixel value of pixel x to $Max(a)$.

Step 3: Reverse the histogram-shifting in the embedding phase for any pixel with a value within the range $Max(a_i)$ to $Min(b_i)$, which can be represented as $x \in (Max(a_i), Min(b_i))$. Then

$$x = \begin{cases} x - 1 & \text{if } Max(a) < Min(b); \\ x + 1 & \text{if } Max(a) > Min(b). \end{cases} \tag{3}$$

Step 4: If there is overhead book-keeping information found in extracted data, set the pixel value of the record pixels, where the position is recorded in the overhead as $Min(b_i)$.

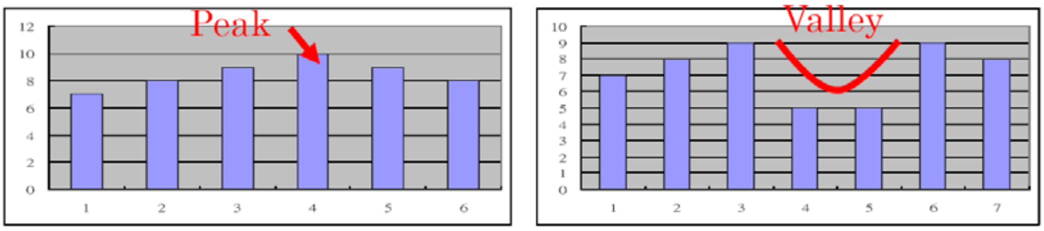
Following the above steps, the cover image can be recovered without any distortion.

3. Steganalytic Features Analysis of Ni et al.'s Reversible Data-Hiding Method.

In terms of developing a discriminator for cover images and stego-images, steganalytic features are the core of steganalysis. In this section, we investigate the differences between cover images and stego-images using the principle of exhaustion, and we propose four significant image features for steganalysis aimed at detecting Ni et al.'s scheme using histograms. The details of the proposed steganalytic features are shown as follows.

***Feature* (0)**: The valley phenomenon.

In this feature, a peak point appears in the portions of the cover image histogram that resemble gentle hills, such as Figure 1(a), where the peak point is located at 4 with 10 pixels in a cover image histogram. A valley phenomenon appears in the corresponding stego-image histogram distribution, as shown in Figure 1(b), where the bottom of the valley is located at pixel values 4 and 5.

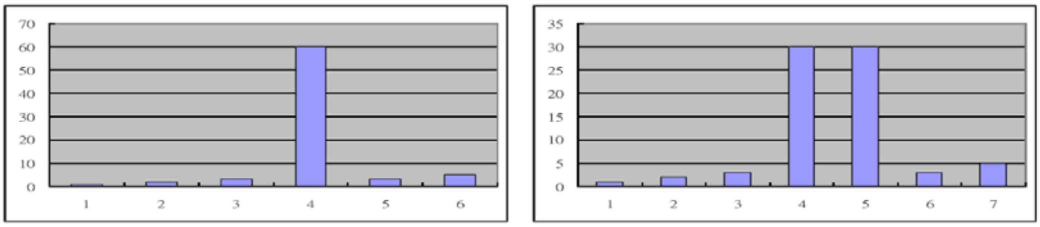


(a) Cover image

(b) Stego-image

FIGURE 1. Feature 0: Valley phenomenon in image histogram

***Feature* (1)**: The skyscraper phenomenon in image histogram.



(a) Cover image

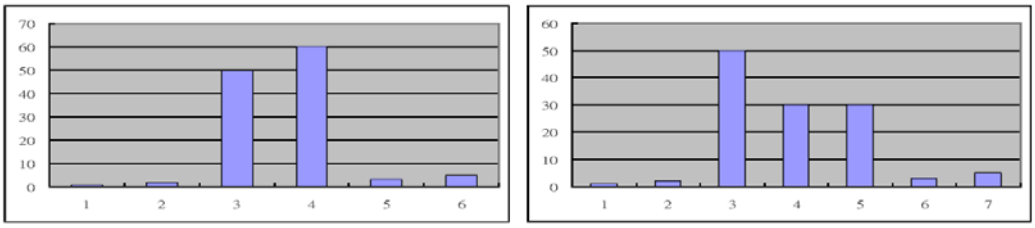
(b) Stego-image

Figure 2. Feature 1: Skyscraper phenomenon in image histogram

Sometimes the pixel number of a peak point appears in the cover image histogram such that it resembles a skyscraper, such as Figure 2(a); in this case, the peak point is located at 4 with 60 pixels in a cover image histogram. Twin skyscrapers appear in the corresponding stego-image histogram distribution, as shown in Figure 2(b) at pixel values 4 and 5.

***Feature*(2)**: The adjoined skyscraper phenomenon in image histogram.

In this feature, the pixel number of a peak point and its (right or left) neighbor resemble twin skyscrapers in the cover image histogram, as in Figure 3(a), where the pixel value of the peak point is equal to 4 with 60 pixels in a cover image histogram. Adjoined twin skyscrapers appear in the corresponding stego-image histogram distribution, as shown in Figure 3(b) at pixel values 4 and 5.



(a) Cover image

(b) Stego-image

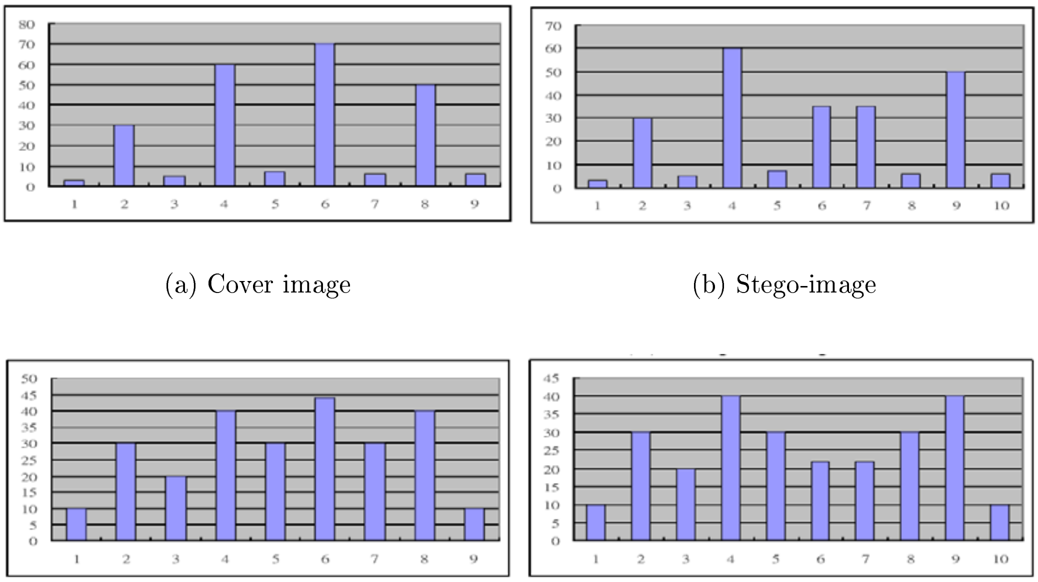
Figure 3. Feature 2: Adjoin-Skyscrapers in image histogram

***Feature*(3)**: The comb phenomenon in image histogram.

This feature occurs when a peak point resembles a comb-like structure in the cover image histogram, such as in Figures 4(a) and 4(c), there the peak point is located at 6 with 70 and 44 pixels in a cover image histogram. A valley-like phenomenon appears in the corresponding stego-image histogram distribution, as shown in Figures 4(b) and 4(d) at pixel values 6 and 7.

From the above-mentioned image histogram analyses, four significant features used to detect Ni et al.'s reversible data-hiding scheme are proposed. According to the proposed steganalytic features, the details of the proposed detection algorithms and procedures are introduced in next section.

4. **The Proposed Feature Coding and Detecting Scheme.** According to the different steganalytic features in Section 3, the features codes are separately generated one-by-one. For a given suspicious image, four features coding the data, which comprise the



(a) Cover image

(b) Stego-image

(c) Cover image

(d) Stego-image

FIGURE 4. Feature 3: Comb phenomenon in image histogram

codebook, can be produced for detecting purposes. The proposed detecting step is as follows. First, generate the Codebook(i) for *Feature*(i) detection. Second, search the *Feature-code*(i) of *Feature*(i). If the *Feature-code*(i) is found in Codebook(i), the suspicious image is detected as a stego-image. If not, continue on to next feature detection step until all features are diagnosed. If no *Feature-code*(i) is found in the corresponding Codebook(i), the suspicious image is undetected. That is, the suspicious image is detected to not be a stego-image. The flowchart of the proposed detection procedure is shown in Figure 5.

The proposed detection method can be simply divided to two parts, namely, histogram features coding and the detection of suspicious images. A method for image feature coding is introduced in Section 4.1, and the implementation of a method to detect suspicious images is discussed in Section 4.2.

4.1. **Histogram feature coding.**

To digitize the information of features introduced in Section 3 to detect the present of data hiding, four codebook-generating algorithms are proposed. Suppose a histogram of a suspicious image S is denoted as H_s, where $H_s(x)$ is the pixel value x in the suspicious grayscale image, $x \in [0, 255]$. The discrete image histogram $H_s(x)$ is treated as a discrete-time signal.

Image feature coding is treated as a digital signal processing procedure. By way of the proposed digital signal processing procedures, namely, sampling and quantification, valuable information (i.e., feature-codes) available for steganalysis is produced. The feature-codes coding algorithms are as follows; there are four algorithms for each of the proposed steganalytic features.

4.1.1. *The Codebook(0) coding algorithm.* Let $C_0[x]$ denote the Codebook(0) of a test image. According to the characteristics of the valley phenomenon, *Feature*(0), the image histogram data $H_s(x)$ is sampled using signal pair x and $x + 1$, where x ranges from 0 to 254.

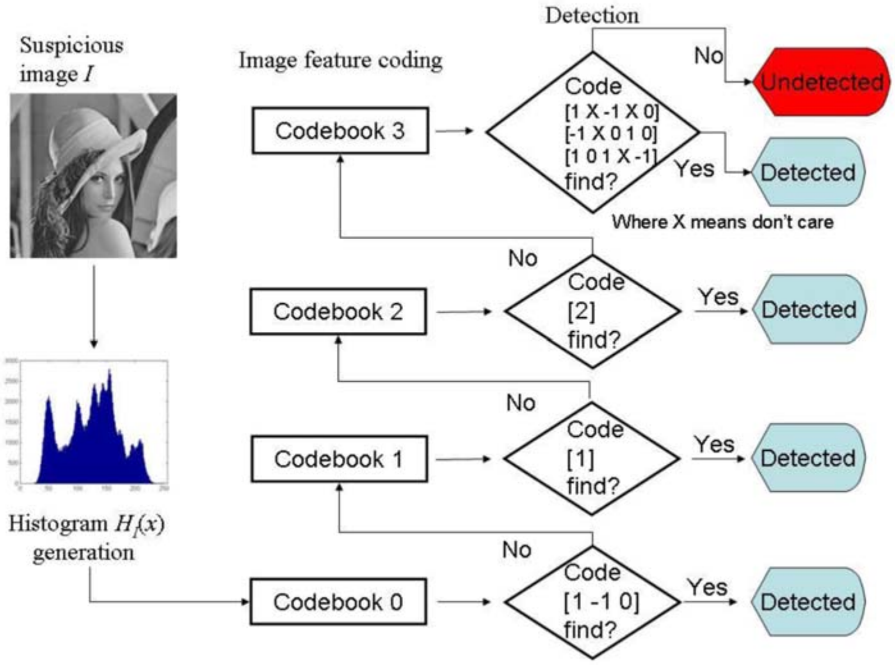


FIGURE 5. Flowchart of the proposed detection procedure

The valley phenomenon can be encoded as follows. If a signal pair is increasing by a threshold τ and $(H_s(x+1) - H_s(x))/H_s(x+1) \geqq \tau$, the quantified Codebook $C_0[x]$ is set to 0, but if a signal pair is decreasing by a threshold τ and $(H_s(x) - H_s(x+1))/H_s(x) \leqq \tau$, the quantified Codebook $C_0[x]$ is set to 1. If the absolute value of a signal pair difference is within the threshold φ and $|H_s(x) - H_s(x+1)|/\max(H_s(x+1), H_s(x) < \varphi$, the quantified Codebook $C_0[x]$ is set to -1. Otherwise, the quantified Codebook $C_0[x]$ is set to 2.

The Feature-code(0) for the valley phenomenon is present as $[1, -1, 0]$. The Feature-code(0) is used to detect the valley phenomenon. In the detection step, the proposed coding algorithm is as follows, where $\tau = 0.1$ and $\varphi = 0.065$.

```
For $x = 0$ to 254
    If $H_s(x+1) - H_s(x) \geqq H_s(x+1) \times \tau$ then $C_0[x] = 0$
    Else if $H_s(x) - H_s(x+1) \leqq H_s(x) \times \tau$ then $C_0[x] = 1$
    Else if $abs(H_s(x) - H_s(x+1)) < (\max(H_s(x+1), H_s(x)) \times \varphi$ then $C_0[x] = -1$
    Else $C_0[x] = 2$
End
```

4.1.2. *The Codebook(1) coding algorithm.* Let $C_1[x]$ denote the Codebook(1) of a test image. Suppose the highest point in an image histogram is located at the pixel value $x_{\max}$. According to the characteristics of the skyscraper phenomenon, *Feature*(1), one skyscraper of two twin skyscrapers in a stego-image-histogram is located at the pixel value $x_{\max}$, while the other is located at the pixel value $x_{\max-1}$.

First, the twin skyscrapers should not locate on gentle hills, as in Figure 2(a); they should be higher than all of their neighbors. If the difference ratio within the area y from $x-2$ to $x+2$ is lower than ε, i.e., $|[H_s(y) - H_s(y+1)]|/H_s(y)] < \varepsilon$, where $y \in [x-2\ x+2]$, then the area y of the histogram is assumed to resemble gentle hills.

Second, the difference ratio between twin skyscrapers should be within a threshold δ; that is, $|[H_s(x_{\max}) - H_s(x_{\max-1})]|/H_s(x_{\max}) < \delta$, and $x_{\max} - x_{\max-1}$ should be equal to 1.

Third, the twin skyscrapers should be higher than neighbors; that is, $|[H_s(x_p) - H_s(x_n)]|/H_s(x_p)] > \zeta$, where $x_p \in [x_{\max}, x_{\max-1}]$, $x_n \in [x_{\max} \pm 1, x_{\max-1} \pm 1]$.

If the twin skyscrapers phenomenon is identified, the feature-code of Codebook $C_1[x]$ is set to 1; otherwise, the Codebook $C_1[x]$ is set to 0. Therefore, the Feature-code(1) of the skyscraper phenomenon is presented as in [1].

The proposed coding algorithm is shown as follows, where $\varepsilon = 0.13$, $\delta = 0.03$ and $\zeta = 0.1$.

```
For $x = 0 \sim 255$

  If $x == x_{\max} \in [2, 253]$

    If $abs((H_s(x_{\max}) - (H_s(x_{\max} + 1))) < (H_s(x_{\max} + 1)) \times \varepsilon$ && $abs((H_s(x_{\max} - 1) - (H_s(x_{\max}))) < (H_s(x_{\max} - 1)) \times \varepsilon$ && $abs((H_s(x_{\max} - 1) - (H_s(x_{\max} - 2))) < (H_s(x_{\max} - 1)) \times \varepsilon$ && $abs((H_s(x_{\max} + 1) - (H_s(x_{\max} + 2))) < (H_s(x_{\max} - 1)) \times \varepsilon$ then $C_1[x] = 0$
    Else if $abs((H_s(x_{\max}) - (H_s(x_{\max} - 1))) < (H_s(x_{\max-1})) \times \delta$ && $x_{\max} - x_{\max-1} = 1$ && $[H_s(x_{\max}) - H_s(x_{\max} - 1) > H_s(x_{\max}) \times \zeta || H_s(x_{\max}) - H_s(x_{\max} + 1) > H_s(x_{\max}) \times \zeta]$ then $C_1[x] = 1$
    End

  Else if $x == x_{\max} \in [0, 1]$

    If $abs(H_s(0) - H_s(1)) < H_s(x_{\max} + 1) \times \zeta/2$ && $abs(H_s(1) - H_s(2)) < H_s(x_{\max} + 1) \times \zeta/2$ then $C_1[x] = 0$
    Else if $abs(H_s(x_{\max}) - H_s(x_{\max-1})) < H_s(x_{\max-1}) \times \delta$ && $abs(x_{\max} - x_{\max-1}) = 1$ then $C_1[x] = 1$
    End

  Else if $x == x_{\max} \in [254, 255]$

    If $abs(H_s(255) - H_s(254)) < H_s(x_{\max} - 1)) \times \zeta/2$ && $abs(H_s(254) - H_s(253)) < (H_s(x_{\max} - 1)) \times \zeta/2$ then $C_1[x] = 0$
    Else if $abs(H_s(x_{\max}) - H_I(x_{\max-1})) < H_s(x_{\max-1}) \times \delta$ && $abs(x_{\max} - x_{\max-1}) = 1$ then $C_1[x] = 1$
    End
  Else $C_1[x] = 2$
  End

End
```

4.1.3. *The Codebook(2) coding algorithm.* Let $C_2[x]$ denote Codebook(2) of a test image. When the twin skyscrapers phenomenon, that is, *Feature*(2), appears in a cover image, as in Figure 4(a), an adjoined skyscrapers phenomenon occurs in the corresponding stego-image, as Figure 4(b) shows.

A lower twin skyscraper is next to the highest skyscraper $H_s(x_{\max})$ in the histogram. In this case, we assume that the difference ratio of the twin skyscrapers is lower than the threshold η, that is, $|[H_s(x_{\max} + 1) - H_s(x_{\max} + 2)]|/H_s(x_{\max} + 1)] < \eta$ or $|[H_s(x_{\max} -$

$1) - H_s(x_{\max} - 2)]|/H_s(x_{\max} - 1)] < \eta$; in addition, the altitude of the adjoined twin skyscrapers should be lower than $\mu\%$ of the highest skyscraper; that is, $[H_s(x_{\max}) - H_s(x_{\max} + 1)]/H_s(x_{\max})] > \lambda$ or $|[H_s(x_{\max}) - H_s(x_{\max} - 1)]|/H_s(x_{\max})] > \lambda$, where $\lambda = 1 - \mu\%$.

If the adjoined skyscrapers phenomenon be identified, the feature-code of Codebook $C_2[x]$ is set as in [2], where $x = x_{\max}$; otherwise, Codebook $C_2[x]$ is set as in [0]. Therefore, the Feature-code(2) of the adjoined skyscraper phenomenon can be depicted as in [2].

The proposed coding algorithm is as follows, where $\eta = 0.05$ and $\lambda = 0.15$.

```
For $x = 0 \sim 255$
  If $x == x_{\max} \in [2, 253]$
    If $abs(H_s(x_{\max}+1) - H_s(x_{\max}+2)) < H_s(x_{\max}+1) \times \eta$ && $abs(H_s(x_{\max}) - H_s(x_{\max}+1)) > H_s(x_{\max}) \times \lambda$ then $C_2[x] = 2$
    Else if $abs(H_s(x_{\max}-1) - H_s(x_{\max}-2)) < (H_s(x_{\max}-1)) \times \eta$ && $abs(H_s(x_{\max}) - H_s(x_{\max}-1)) > (H_s(x_{\max})) \times \lambda$ then $C_2[x] = 2$
  End
  Else if $x == x_{\max} \in [0, 1]$
    If $abs(H_s(0) - H_s(1)) < H_s(x_{\max}+1) \times \eta$ && $abs(H_s(2) - H_s(3)) < (H_s(x_{\max}+1)) \times \eta$ then $C_2[x] = 0$
    Else if $abs(H_s(x_{\max}+1) - H_s(x_{\max}+2)) < (H_s(x_{\max}+1)) \times \eta$ then $C_2[x] = 2$
    End
  Else if $x == x_{\max} \in [254, 255]$
    If $abs(H_s(254) - H_s(255)) < H_s(x_{\max}-1)) \times \eta$ && $abs(H_s(253) - H_s(254)) < H_s(x_{\max}-1)) \times \eta$ then $C_2[x] = 0$
    Else if $abs(H_s(x_{\max}-1) - H_s(x_{\max}-2)) < H_s(x_{\max}-1) \times \eta$ then $C_2[x] = 2$
    End
  Else $C_2[x] = 0$
  End
End
```

4.1.4. *The Codebook(3) coding algorithm.* Let $C_3[x]$ denote the Codebook(3) of a test image. When the comb phenomenon, that is, *Feature*(3), appears in a cover image, the high and low peaks in a histogram are interlaced, such as in Figures 5(a) and 5(c). The corresponding histogram distributions of the stego-images are shown in Figures 5(b) and 5(d).

According to the characteristics of the comb phenomenon, the image histogram datum $H_s(x)$ is sampled using signal pair of x and $x + 1$, where x ranges from 0 to 254. If a signal pair increases by a threshold ρ, where $(H_s(x + 1) - H_s(x))/H_s(x + 1) > \rho$, the quantified codebook $C_3[x]$ is set to 0; if a signal pair decreases by a threshold ρ, where $(H_s(x) - H_s(x + 1))/H_s(x) > \rho$, the quantified codebook $C_3[x]$ is set to 1. If the absolute value of the difference in the signal pair is within the threshold φ, where

$|H_s(x) - H_s(x+1)|/\max(H_s(x+1), H_s(x)) \leqq \varphi$, the quantified codebook $C_3[x]$ is set to -1. Otherwise, the quantified codebook $C_3[x]$ is set to 2.

Therefore, the comb phenomenon is present as $[1, X, -1, X, 0]$, $[-1, X, 0, 1, 0]$ or $[1, 0, 1, X, -1]$, where X is a placeholder that can be filled with any value.

The proposed coding algorithm is shown as follows, where $\rho = 0.065$ and $\varphi = 0.065$.

```
For $x = 0 \sim 254$
  If $H_s(x+1) - H_s(x) > H_s(x+1) \times \rho$ then $C_3[x] = 0$
  Else if $H_s(x) - H_s(x+1) > H_s(x) \times \rho$ then $C_3[x] = 1$

  Else if $abs(H_s(x) - H_s(x+1)) \leqq \max(H_s(x+1), H_s(x)) \times \varphi$ then $C_3[x] = -1$

  Else $C_3[x] = 2$
End
```

4.2. **The detection of suspicious images.** The detection procedure involves searching the feature-code patterns from the produced codebooks one-by-one until the steganalytic results are returned. If a proposed steganalytic feature is found among the features is introduced in Section 3, the suspicious image is classified as a stego-image. Otherwise, the suspicious image is determined to not a stego-image. The details of feature-code searching are shown in the following steps.

Step 1: ***Feature*(0) detection**: First, generate Codebook(0) for the suspicious image. Second, if the suspicious image is determined to be a stego-image, the following rules should be satisfied.

1. $\forall x_d \in [0\ 253] : C_0[x_d, x_d+1, x_d+2] =$ Feature-code(0), where Feature-code(0) $= [1, -1, 0]$.
2. $\forall x_d \in [0\ 253] : H_s(x_d + f) > \frac{1}{10} \sum_{w=0}^{4} H_s(x_{\max -w})$, where $f = 1$ and 2. $x_{\max -w}$ represents the $(w+1)$th highest bar in the image histogram.
3. $\forall x_d \in [0\ 253] : H_s(x_d) > H_s(x_{\max -9})$ or $\forall x_d \in [0\ 253] : H_s(x_d + 3) > H_s(x_{\max -9})$.
4. $\forall x_d \in [0\ 252] : \frac{H_s(x_d) - H_s(x_d+1)}{H_s(x_d)} > 0.35$ and
   $\forall x_d \in [0\ 252] : \frac{H_s(x_d+3) - H_s(x_d+2)}{H_s(x_d+3)} > 0.35$.

In addition, while rules 1 and 2 must be obeyed, either rule 3 or 4 must be fulfilled. If the features of the suspicious image do not conform to the above-mentioned rules, generate Codebook(1) and continue the following steps.

Step 2: ***Feature*(1) detection**: If feature-code(1) is found in Codebook(1), the suspicious image is determined to be a stego-image. Otherwise, continue to the next step.

Step 3: ***Feature*(2) detection**: If feature-code(2) is found in Codebook(2), the suspicious image is determined to be a stego-image. Otherwise, continue to the next step.

Step 4: ***Feature*(3) detection**: The comb phenomenon can be indicated by three different types of Feature-code$(3, j)$, namely, $[1, X, -1, X, 0]$, $[-1, X, 0, 1, 0]$ and $[1, 0, 1, X, -1]$, where $j = 1, 2, 3$. If one of these three types is found, the suspicious image is determined to be a stego-image. The three different cases for the three different codes are shown as follows.

Case $[\mathbf{1}, \mathbf{X}, -\mathbf{1}, \mathbf{X}, \mathbf{0}]$: If a suspicious image is determined to be a stego-image, all of the following rules should be satisfied.

1. $\forall x_d \in [0\ 251] : C_3[x_d, x_d + 1, x_d + 2, x_d + 3, x_d + 4] =$ Feature-code(3, 1), where Feature-code$(3, 1) = [1, X, -1, X, 0]$, and X is simply a placeholder for any value.
2. $\forall x_d \in [0\ 251] : H_s(x_d + g) > \dfrac{1}{10} \sum_{w=0}^{4} H_s(x_{\max - w})$, where $g = 2$ and 3. $x_{\max - w}$ represents the $(w + 1)$th highest bar of the image histogram.
3. $\forall x_d \in [0\ 251] : H_s(x_d) > H_s(x_{\max - 9})$ or $\forall x_d \in [0\ 250] : H_s(x_d + 5) > H_s(x_{\max - 9})$.
4. $\forall x_d \in [0\ 251] : \dfrac{|H_s(x_d) - H_s(x_d + 2)|}{H_s(x_d + 1)} > 0.35$.

Case $[-\mathbf{1}, \mathbf{X}, \mathbf{0}, \mathbf{1}, \mathbf{0}]$: If a suspicious image is determined to be a stego-image, all of the following rules should be satisfied.

1. $\forall x_d \in [0\ 251] : C_3[x_d, x_d{+}1, x_d{+}2, x_d{+}3, x_d{+}4] =$ Feature-code(3, 2), where Feature-code$(3, 2) = [-1, X, 0, 1, 0]$, and X is simply a placeholder for any value.
2. $\forall x_d \in [0\ 251] : H_s(x_d + h) > \dfrac{1}{10} \sum_{w=0}^{4} H_s(x_{\max - w})$, where $h = 0$ and 1. $x_{\max - w}$ represents the $(w + 1)$th highest bar of the image histogram.
3. $\forall x_d \in [0\ 251] : H_s(x_d + 3) > H_s(x_{\max - 9})$.
4. $\forall x_d \in [0\ 251] : \dfrac{|H_s(x_d + 1) - H_s(x_d + 2)|}{H_s(x_d + 2)} > 0.35$.
5. $\forall x_d \in [0\ 251] : \dfrac{|H_s(x_d) - H_s(x_d + 2)|}{H_s(x_d + 1)} > 0.35$.

Case $[\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{X}, -\mathbf{1}]$: If a suspicious image is determined to be a stego-image, all of the following rules should be satisfied.

1. $\forall x_d \in [0\ 251] : C_3[x_d, x_d + 1, x_d + 2, x_d + 3, x_d + 4] =$ Feature-code(3, 3), where Feature-code$(3, 3) = [1, 0, 1, X, -1]$, and X is simply a placeholder for any value.
2. $\forall x_d \in [0\ 251] : H_s(x_d + k) > \dfrac{1}{10} \sum_{w=0}^{4} H_s(x_{\max - w})$, where $k = 4$ and 5, $x_{\max - w}$ represents the $(w + 1)$th highest bar of the image histogram.
3. $\forall x_d \in [0\ 251] : H_s(x_d + 2) > H_s(x_{\max - 9})$.
4. $\forall x_d \in [0\ 251] : \dfrac{|H_s(x_d + 4) - H_s(x_d + 3)|}{H_s(x_d + 3)} > 0.35$.

Following the above steps, if a suspicious image is not determined to be a stego-image, the suspicious image is classified as an original image. The details of the experimental results with respect to the implementation of proposed detection method are shown in the next section.

5. Experimental Results.

We downloaded 1,338 original test images from the Uncompressed Colour Image Database (UCID) web site [15]. All 1,338 color images were transformed into an 8-bit grayscale format to serve as test cover images. Matlab 7.6 was used to implement the proposed steganalysis method. The embedded secret messages were generated randomly by a pseudo-random number generator.

To reduce the complexity of the experiments, the choice of reversible key in the experiments is depended on following rules. In the one-pair case, select a hiding pair consisting of a peak point and a zero point in the pixel value range of R from 0 to 255. In the two-pair case, one hiding pair is selected in the pixel value range of R from 0 to 127, and another hiding pair is selected in the pixel value range of R from 128 to 255. In the three-pair case, the first hiding pair is selected in the pixel value range of R from 0 to 84, and the second hiding pair is selected in the pixel value range of R from 85 to 169. The third hiding pair is selected in the pixel value range of R from 170 to 255.

Recently, multilevel data-hiding schemes have been introduced to improve data-hiding capacity. These multilevel data-hiding schemes embed secret messages using a specific data-hiding algorithm repeatedly, meanwhile maintaining an acceptable level of distortion. These methods can be used to improve Ni et al.'s reversible data-hiding method as well. Therefore, this approach is included in our experiments. A total of 8,028 test images consisting of 1,338 original cover images and 6,690 stego-images generated by Ni et al.'s data-hiding scheme with different hiding pairs and at different levels are tested. The stego-images have a number of hiding pairs ranging from 1 to 3, and each hiding pair case consists of 1,338 stego-images. In the multilevel data-hiding scheme, the number of hiding pairs is set to 1, while the level is set to 2 or 3. Each hiding level case consists of 1,338 stego-images.

The capacity comparisons of 8 standard grayscale 512×512×8 test images (Figure 6) between the two schemes (i.e., multi-pair versus multilevel data-hiding schemes) are shown in Table 1. The embedding capacity of the two schemes highly depends on the amount of peak points. This is because the multilevel data-hiding scheme always chooses the maximum points in an image histogram to embed message, but multi-pairs scheme do not. Therefore, the embedding capacity of multilevel data-hiding scheme is generally higher than multi-pairs schemes.

Figure 6. Eight standard grayscale 512×512×8 test images

The performance of a steganalytic system can be simply estimated using four parameters, namely, true-positive (TP), false-positive (FP), true-negative (TN) and false-negative (FN) indicators. True-positive (TP) indicates the number of stego-images that are correctly identified, while false-positive (FP) indicates the number of cover images that are incorrectly identified as stego-images. True-negative (TN) indicates the number of cover images that are correctly identified, and false-negative (FN) indicates the number of stego-images that are incorrectly identified as cover images. Hence, better steganalytic systems are expected to obtain higher values for TP and lower values for FP. Assume the number of tested images is Φ, and the number of correctly identified images is θ. The standard definition of detection accuracy is the percentage of correctly identified cover

Table 1. Capacity comparisons of different grayscale-images embedding

Capacity **Test image**	**1 pairs V.S. 1 level (bits)**		**2 pairs V.S. 2 level (bits)**		**3 pairs V.S. 3 level (bits)**	
Lena	2748	2748	4973	5457	6154	8141
Aerial	5173	5173	5694	10128	7464	14962
Baboon	2759	2759	5318	5499	6367	8217
Boat	5394	5394	6875	10546	12027	15473
Frog	26098	26098	46483	46483	34031	64915
Goldhill	2618	2618	4676	5178	6111	7689
Peppers	2950	2950	5224	5898	7202	8816
Zelda	2588	2588	4844	5142	4843	7692
Average bps	**0.024**	**0.024**	**0.040**	**0.045**	**0.040**	**0.064**

and stego-images, i.e.,

$$\boldsymbol{Detection\ accuracy} = \theta/\Phi.$$

In the experiments, a total of 8,028 grayscale images were tested. The experimental detection results are shown in Table 2. The average detection accuracy for cover images is 91.48%; for multi-pairs data-hiding schemes with 1 to 3 pairs, it is 88.33%, while for multilevel data-hiding schemes with 1 to 3 levels, it is 87.25%. From the experimental results, the proposed steganalytic method is efficient at detecting Ni et al.'s reversible data-hiding scheme.

Table 2. Detection results

Tested images	***TN***	***FP***	***Accuracy***
Cover image	1224	114	91.48%
Tested images	***TP***	***FN***	***Accuracy***
1-pair (1-level) stego image	1139	199	85.13%
2-pairs stego image	1192	146	89.09%
3-pairs stego image	1197	141	89.46%
2-level stego image	1223	115	91.41%
3-level stego image	1121	217	83.78
Multi-pairs detection average accuracy		**88.33%**	
Multilevel detection average accuracy		**87.25%**	
Overall accuracy		**87.79%**	

We examined the images that were misclassified and noted that the histogram distributions of those cover images that were detected as stego-images have features similar to the features of stego-images identified above. A similar situation occurs also for stego-images; because of the diversity of images, some histogram features of stego-images may be resistant to our steganalysis method. Most of the misclassified images do not have obvious types or characteristics, which poses a challenge for future work.

6. Conclusions.

Thus far, no effective steganalytic method has been proposed to detect Ni et al.'s reversible data-hiding scheme. In this paper, we investigate several different histogram features between cover images and stego-images and propose a novel steganalysis method based on histogram feature coding. Based on an analysis of image histograms, four significant steganalytic features are identified to differentiate between cover images and stego-images. These histogram features of stego-images are characterized using four kinds of feature codes. Using the proposed detection method, we are able to distinguish stego-images from cover images with an overall accuracy of 87.79%. The experimental results show that the proposed method is efficient in detecting the use of Ni et al.'s dating-hiding method, including both multi-pair data-hiding schemes as well as multilevel data-hiding schemes.

Acknowledgements. This work was supported partially by the National Science Council of Taiwan under grant NSC 98-2221-E-182-066-MY2. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] W.-L. Tai and C.-C. Chang, Data hiding based on VQ compressed images using hamming codes and declustering, *International Journal of Innovative Computing, Information and Control*, vol.5, no.7, pp.2043-2052, 2009.

[2] M.-H. Tsai, Y.-B. Lin and C.-M. Wang, Image sharing with steganography and cheater identification, *International Journal of Innovative Computing, Information and Control*, vol.6, no.3(A), pp.1165-1178, 2010.

[3] C.-C. Lin, Y.-H. Chen and C.-C. Chang, LSB-based high-capacity data embedding scheme for digital images, *International Journal of Innovative Computing, Information and Control*, vol.5, no.11(B), pp.4283-4289, 2009.

[4] C.-C. Chang, T.-C. Lu, Y.-F. Chang and C.-T. Lee, Reversible data hiding schemes for deoxyribonucleic ACID (DNA) medium, *International Journal of Innovative Computing, Information and Control*, vol.3, no.5, pp.1145-1160, 2007.

[5] T.-C. Lu and C.-H. Tsai, An improved lossless hiding technique using integer transformation function, *International Journal of Innovative Computing, Information and Control*, vol.5, no.9, pp.2645-2656, 2009.

[6] C.-S. Chan and C.-Y. Chan, Reversible data hiding in two steganographic images using matrix coding, *International Journal of Innovative Computing, Information and Control*, vol.6, no.5, pp.2089-2102, 2010.

[7] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, Reversible data hiding, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.16, no.3, pp.354-362, 2006.

[8] X.-Y. Luo, D.-S. Wang, P. Wang and F.-L. Liu, A review on blind detection for image steganography, *Signal Processing*, vol.88, no.9, pp.2138-2157, 2008.

[9] C.-N. Bui, H.-Y. Lee, J.-C. Joo and H.-K. Lee, Steganalysis method defeating the modified the modified pixel-value differencing steganography, *International Journal of Innovative Computing, Information and Control*, vol.6, no.7, pp.3193-3203, 2010.

[10] S. Dumitrescu, X. Wu and Z. Wang, Detection of LSB steganography via sample pair analysis, *IEEE Transactions on Signal Processing,* vol.51, no.7, pp.1995-2007, 2003.

[11] D.-C. Lou, C.-L. Lin and C.-L. Liu, Universal steganalysis scheme using support vector machine, *Optical Engineering*, vol.46, no.11, pp.117002-1-117002-10, 2007.

[12] Y. Wang and P. Moulin, Optimized feature extraction for learning-based image steganalysis, *IEEE Transactions on Information Forensics and Security*, vol.2, no.1, pp.31-45, 2007.

[13] D.-D. Fu, Y.-Q. Shi, D.-K. Zou and G.-R. Xuan, JPEG steganalysis using empirical transition matrix in block DCT domain, *Proc. of IEEE International Workshop on Multimedia Signal Processing*, pp.310-313, 2006.

[14] W.-C. Kuo and Y.-H. Lin, On the security of reversible data hiding based-on histogram shift, *Proc. of the 3rd International Conference on Innovative Computing, Information and Control*, Dalian, China, pp.174-178, 2008.

[15] *Uncompressed Colour Image Database*, http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html, 2010.