Detection of Reversible Data Hiding Scheme Based on Histogram Feature Codes

Der-Chyuan Lou
Department of Computer Science and Information Engineering,
Chang Gung University,
Taoyuan, Taiwan
dclouprof@gmail.com

Chen-Hao Hu, Chung-Cheng Chiu, and Te-Jen Chang
Department of Electrical Engineering,
Chung Cheng Institute of Technology,
National Defense University,
Taoyuan, Taiwan
chenhao.hu@gmail.com; davidchiu@ndu.edu.tw;
karl591218@gmail.com

***Abstract*—Reversible data hiding scheme assures that the original cover image can be totally recovered from the stego-image after the hidden messages are extracted. Those techniques are suitable for the applications of military, medical, high-energy particle physical experimental investigation and artistic purposes when any distortion to the original images is not acceptable. In 2006, Ni et al. proposed a reversible data hiding algorithm base on histogram shifting. Utilizing the zero or minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed messages into the image. The goal of steganalysis is to identify suspected images, determine whether or not they have messages embedded in them. In this paper, a novel steganalytic scheme against Ni et al.'s steganographic method based on histogram feature codes is proposed. Experimental results show that the steganalytic scheme is capable to detect the Ni *et al.*s' steganographic method.**

***Index Terms*—reversible data hiding, steganography, steganalysis, histogram.**

I. Introduction

Data hiding [1] is a process to conceal secret messages in a cover media and make it can't be detectable. Reversible data hiding techniques [2-4] provide not only conceal the secret messages in a cover media but also lossless reconstruct the original cover media after the extracting of the secret messages. Reversible data hiding techniques satisfy some applications those without any distortion of the cover media, such as military, medical, high-energy particle physical experimental investigation and artistic purposes.

In contrary to data hiding, the goal of steganalysis is detecting the present of secret messages, even determining the steganographic methods. Current steganalysis techniques [5] fall broadly into one of two categories: specific [6, 7] or universal blind steganalysis [8, 9]. Specific steganalysis can examine the present of a secret message embedded by specific steganographic algorithm, or even can estimate the embedding ratio. Universal blind steganalysis is a meta-detection method in the sense that it can be adjusted, after training on lots of original and stego-medias, to detect most of well-know steganographic methods. In general, steganalysis methods target a specific embedding method can give more accurate and reliable results than any universal blind steganalysis.

In 2006, Ni. *et al*. proposed a reversible data hiding algorithm based on histogram shifting [10], with low computational complexity and short execution time. In this paper, we investigate the difference of histogram features between cover images and stego-images. Then, a novel specific steganalysis method against Ni. *et al*.s' reversible data hiding algorithm is proposed. Through the proposed sampling and quantifying processes, the image histogram feature codes are encoded. According to the histogram feature codes, the stego-images are detectable from the original ones.

II. Review of The Ni *et. al*.s' Reversible Data Hiding Scheme

The Ni *et al*.s' reversible data hiding scheme [10] can be concluded in following steps.

Step 1. Find k pairs of maximum points $Max(a)$ and

minimum points *Min*(*b)* of histogram of a cover image. Deal with each pair using following steps, one by one.

Step 2. Set minimum points as zero points. If the pixel values of these minimum points are not equal to zero, set the pixel values of minimum points be zero and record the positions of these pixels as overhead bookkeeping information. That is in order to recover these pixels in data extraction steps and get the original cover image back.

Step 3. Without loss of generality, assume the pixel values of one pair of maximum and minimum points $P(Max(a)) < P(Min(b))$. If the pixel value of a cover image $P(I) = x$, where $x \in (P(Max(a)), P(Min(b)))$, then $P(I) = x + 1$. Otherwise, when $P(Max(a)) > P(Min(b))$, if $P(I) = x$, where $x \in (P(Max(a)), P(Min(b)))$, then $P(I) = x - 1$.

Step 4. Scan the cover image in some sequential order and embedding data *m* (messages and overhead) by replace the pixel values of *Max*(*a*) sequentially as follows.

- When $P(Max(a)) < P(Min(b))$, if $m = 1$ then $P(Max(a)) = P(Max(a)) + 1$, else keep $P(Max(a))$ unchanged.
- When $P(Max(a)) > P(Min(b))$, if $m = 1$ then $P(Max(a)) = P(Max(a)) - 1$, else keep $P(Max(a))$ unchanged.

In data extraction process, suppose all pairs of maximum and minimum points *a* and *b* are known, the multiple pairs case can be treated as the multiple repletion of the data extraction for one pair case. Extraction process can be concluded in following steps.

Step 1. Scan the marked image in the same sequential order as the embedding procedure. If the value of a pixel is equal to $a+1$, a bit "1" is extracted. If the value of a pixel is equal to *a*, a bit "0" is extracted.

Step 2. Scan the image again, for any pixel whose value $x \in (a, b]$,

- When $a < b$, $x = x - 1$.
- When $a > b$, $x = x + 1$.

Step 3. If there is overhead bookkeeping information found in extracted data, set the pixel value (whose position is recorded in the overhead) as *b*.

In this way, the cover image can be recovered without any distortion.

III. Histogram Feature Codes And The Proposed Detecting Algorithm

According to the histogram features of stego-images those produced by Ni *et al*.s' reversible data hiding scheme, two samples of the differences between cover image and stego-image are shown in Fig. 1 and Fig. 2. We introduce some feature codes for detection and propose the detecting method. The detection method can be simply divided to three steps: histogram generation, feature codes generation, and detection of suspicious image. The proposed scheme is shown as follows.

Step 1. Histogram generation: Suppose a histogram of a suspicious image *I* noted as H_I and $H_I(x)$ is the number of pixel value *x* of the suspicious image, where $x \in 0 \sim 255$.

Step 2. Feature codes generation:

Code 0:

When $H_I(x+1) - H_I(x) >= H_I(x+1)*0.1$
then $C_0[x] = 0$,

When $H_I(x+1) - H_I(x) <= H_I(x+1)*0.1$
then $C_0[x] = 1$,

When $abs(H_I(x+1) - H_I(x)) < (max(H_I(x+1), H_I(x))*0.065$
then $C_0[x] = -1$.

Code 1:

When $x \sim= x_{max}$ then $C_1[x] = 0$,

When $x = x_{max} = [2, 253]$ && $abs((H_I(x_{max}) - (H_I(x_{max}+1))) < (H_I(x_{max}+1))*0.13$ && $abs((H_I(x_{max}-1) - (H_I(x_{max}))) < (H_I(x_{max}-1))*0.13$ && $abs((H_I(x_{max}-1) - (H_I(x_{max}-2))) < (H_I(x_{max}-1))*0.13$ &&

$abs((H_I(x_{max}+1) - (H_I(x_{max}+2))) < (H_I(x_{max}-1))*0.13$

then $C_1[x] = 0$,

When $x = x_{max} = [2, 253]$ && $abs((H_I(x_{max}) - (H_I(x_{max}+1))) < (H_I(x_{max}))*0.03$ || $abs((H_I(x_{max}) - (H_I(x_{max}-1))) < (H_I(x_{max}))*0.03$

then $C_1[x] = 1$,

When $x = x_{max} = [0, 1]$ && $abs((H_I(0) - (H_I(1))) < (H_I(x_{max}+1))*0.05$ && $abs((H_I(2) - (H_I(3))) < (H_I(x_{max}+1))*0.05$

then $C_1[x] = 0$,

When $x = x_{max} = [0, 1]$ && $abs((H_I(x_{max}) - (H_I(x_{max-1}))) < (H_I(x_{max-1}))*0.03$ && $abs(x_{max} - x_{max-1}) = 1$

then $C_1[x] = 1$,

When $x = x_{max} = [254, 255]$ && $abs((H_I(255) - (H_I(254))) < (H_I(x_{max-1}))*0.05$ && $abs((H_I(254) - (H_I(253))) < (H_I(x_{max-1}))*0.05$

then $C_1[x] = 0$,

When $x = x_{max} = [254, 255]$ &&$abs((H_I(x_{max}) - (H_I(x_{max-1}))) < (H_I(x_{max-1}))*0.03$ && $abs(x_{max} - x_{max-1}) = 1$

then $C_1[x] = 1$.

Code 2:

When $x \sim= x_{max}$ then $C_2[x] = 0$,

When $x = x_{max} = [2, 253]$ && $abs((H_I(x_{max}+1) - (H_I(x_{max}+2))) < (H_I(x_{max}+1))*0.05$ && $abs((H_I(x_{max}) - (H_I(x_{max}+1))) > (H_I(x_{max}))*0.15$

then $C_2[x] = 2$,

When $x = x_{max} = [2, 253]$ && $abs((H_I(x_{max}-1) - (H_I(x_{max}-2))) < (H_I(x_{max}-1))*0.05$ && $abs((H_I(x_{max}) - (H_I(x_{max}-1))) > (H_I(x_{max}))*0.15$

then $C_2[x] = 2$,

When $x = x_{max} = [0, 1]$ && $abs((H_I(0) - (H_I(1))) < (H_I(x_{max}+1))*0.05$ && $abs((H_I(2) - (H_I(3))) < (H_I(x_{max}+1))*0.05$

then $C_2[x] = 0$,

When $x = x_{max} = [0, 1]$ && $abs((H_I(x_{max}+1) - (H_I(x_{max}+2))) < (H_I(x_{max}+1))*0.05$

then $C_2[x] = 2$,

When $x = x_{max} = [254, 255]$ && $abs((H_I(254) - (H_I(255))) < (H_I(x_{max}-1))*0.05$ && $abs((H_I(253) - (H_I(254))) < (H_I(x_{max}-1))*0.05$

then $C_2[x] = 0$,

When $x = x_{max} = [254, 255]$ && $abs((H_I(x_{max}-1) - (H_I(x_{max}-2))) < (H_I(x_{max}-1))*0.05$

then $C_2[x] = 2$.

Code 3:

When $H_I(x+1) - H_I(x) > H_I(x+1)*0.065$

then $C_3[x] = 0$,

When $H_I(x+1) - H_I(x) < -H_I(x)*0.065$ then $C_3[x] = 1$,

When $abs(H_I(x+1) - H_I(x)) <= (max(H_I(x+1), H_I(x))*0.065$

then $C_3[x] = -1$.

Step 3. Detection procedure: The procedures of the proposed detection scheme can be divided into five steps as follows, flowchart is shown in Fig 3.

A. Generate the histogram of a suspicious im-

age.

B. Generate codebook Code 0 of the histogram: If code [1 -1 0] is found in codebook Code 0 $C_0[x]$, the suspicious image is determined as a stego-image. Otherwise, continue next step.

C. Generate codebook Code 1 of the histogram: If code [1] is found in codebook Code 1 $C_1[x]$, the suspicious image is determined as a stego-image. Otherwise, continue next step.

D. Generate codebook Code 2 of the histogram: If code [2] is found in codebook Code 2 $C_2[x]$, the suspicious image is determined as a stego-image. Otherwise, continue next step.

E. Generate codebook Code 3 of the histogram: If code [1 X -1 X 0], [-1 1 0 1 0], and [1 0 1 0 -1] are found in codebook Code 3 $C_3[x]$, the suspicious image is determined as a stego-image. Otherwise, the suspicious image is not a stego-image.

IV. Experimental Results and Conclusions

In this section, we present the results obtained from the experiments of the proposed scheme. In the experiments, we downloaded 1,338 images from image databases [11]. All of which were transformed into an 8-bit grayscale format to act as the test cover images. The hidden messages are random bits produced by a pseudo-random-number generator. 1,338 original cover images and 1,338 stego-images are applied to the detection scheme. Let hiding pairs be equal to one - three pairs. The detection results are shown in Table 1. There are 114/1,338 cover images are determined as stego-images in all case. In one pair case, there are 1,152/1,338 stego-images are positive detected. In other case, there are 1,213/1,338 and 1,098/1,338 stego-images are positive detected relatively.

In this paper, a specific steganalysis scheme based on histogram feature codes is proposed. The steganalysis experiments show that the proposed method received good performance. The future work will focus on the detection of other reversible data hiding methods based on histogram shifting, and the range of the pixel values of hiding bits.

Acknowledgements

This work was supported partially by the National Science Council of Republic of China under grant NSC 98-2221-E-182-066-MY2.

Reference

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, No. 3&4, pp.331-336, 1996.

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253-266, Feb. 2005.

[3] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp.321-330, Sept. 2007.

[4] P. Tsai, Y.-C. Hu, and H.-L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129-1143, June 2009.

[5] 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, Sept. 2008.

[6] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22-28, Oct.-Dec. 2001.

[7] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," *Proceedings of the Third International Workshop Information Hiding*, Dresden, Germany, Sep. 28-Oct. 1, 1999, pp. 61-76.

[8] 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, Nov. 2007.

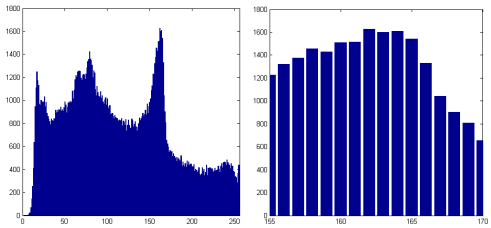
[9] D.-C. Lou, C.-L. Lin, and J.-L. Liu, "Novel steganalysis schemes for BPCS steganography," *The Imaging Science Journal*, vol. 56, no. 4, pp. 232-242, Aug. 2008.

[10] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transaction on Circuits Systems Video Technology*, vol. 16, no.

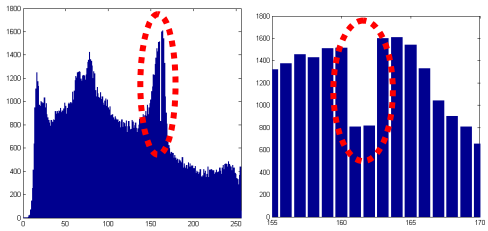
3, pp. 354-362, March 2006.

[11] Uncompressed Colour Image Database, http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html, Oct. 2009.

(a) Chair



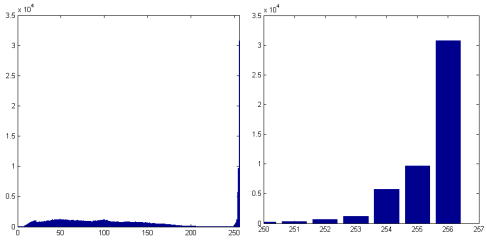
(b) Histogram of cover image of Chair



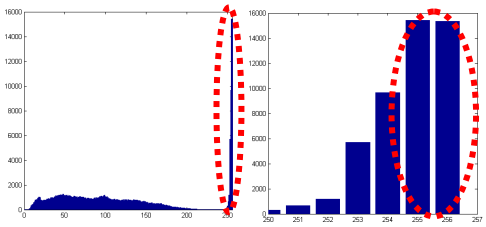
(c) Histogram of stego-image Chair

Figure 1. The differences between cover image and stego-image of Chair.

(a) Buildings



(b) Histogram of cover image Buildings



(c) Histogram of stego-image Buildings

Figure 2. The differences between cover image and stego-image Buildings.

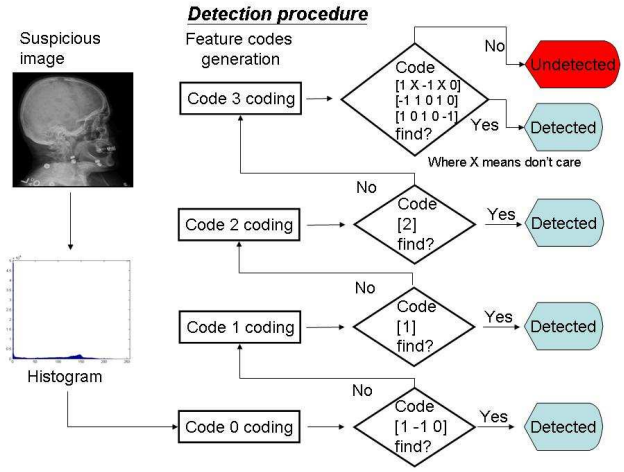


Figure 3. Flowchart of the proposed detection procedure.

Table 1. Detection results.

Hiding pairs	Cover image		Stego-image	
	Positive	%	Positive	%
1	114	0.0852	1152	0.8610
2	114	0.0852	1213	0.9066
3	114	0.0852	1098	0.8206
Average ratio		0.0852		0.8627