Steganalysis of Reversible Contrast Mapping Watermarking

Yeh-Shun Chen, *Ran-Zan Wang, Yeuan-Kuen Lee, Shih-Yu Huang

***Abstract*—This paper proposes a steganalysis scheme for detecting the reversible contrast mapping (RCM) watermarking [1]. In the RCM watermarking scheme, the pixel pairs belonging to the RCM domain are transformed where artifacts are introduced to the least significant bits in the marking process. Through analysis, we find the histogram of LSB varies from a stego-image to the cover image. Based on this observation, we design a specific steganalytic method for cracking the RCM watermarking. Experiment results show the detection accuracies of the RCM watermarking with various embedding rates are acceptable. It can be applied in detecting the misuse of steganographic technology in malicious activities.**

Index Terms—Reversible Contrast Mapping, Steganalysis, Steganography, Watermarking

I. INTRODUCTION

Steganography [1−3] is the art and science of concealed communication. The basic concept is to hide the very existence of the secret message. Digital object such as a text, image, video, or audio segment can be used as the cover data. The camouflaged object, called the stego-data, carries the secret message silently to the recipient. It is essential that the stego-data works as usual likes a normal standard cover data does, hence not to attract the attentions of unintended users. To obtain acceptable hiding payload and keep the fidelity of the stego-image, LSB-based embedding techniques [4,5] are popular and widely studied in the literature. Given that human eyes are most sensitive to edges, these methods usually hide more data in image areas with higher spatial variations. Reversible steganography [1,5−7] is one of the interesting branches of steganographic technology in which the original cover image can be reconstructed without any loss. It addresses an approach for conceal communication in sensitive images such as medical or military images. Literature reports show many methods such as difference expansion [6], histogram shift [7] and generalized-LSB [5] can be used to manage the spare space for embedding data. Recently, Coltuc et al. [1] proposed a reversible contrast mapping (RCM) watermarking scheme that is fast and has a high hiding-payload. It hides the message only in those pixel pairs of an image belonging to the RCM domain, hence provides the ability of perfectly reconstruction of the original cover image.

In the past, much attention has been given on designing steganographic schemes to ensure the secrecy of confidential covert communication. To prevent misuse of these methods in malicious activities, effective steganalysis methods [8−10] that can detect the hidden messages are necessary. In general, steganalysis methods can be classified into two groups: a passive class and another active class. Methods belonging to the first class aim to detect the very existence of secret message, while methods in the second class not only have the detecting ability but also can extract some useful information for further analyses.

In this paper, we propose a steganalytic scheme to detect the RCM watermarking scheme. The positive experimental results show the feasibility of the proposed method. It is useful in detecting malicious activities on stego-images, and also suggests a design consideration for future development of steganographic techniques. The rest of this paper is organized as follows. The RCM watermarking scheme is first reviewed in the next section. Section III describes the proposed steganalytic scheme. Experimental results are presented in Section IV, and conclusions are made finally in Section V.

II. REVIEW OF THE RCM WATERMARKING SCHEME

In the steganographic method proposed in [1], a simple reversible integer to integer transformation called reversible contrast mapping (RCM) is defined and applied to select pixels for embedding embed data. Without loss of generality, for a t-bit image, and (a,b) be a pair of pixels. The forward RCM is defined below:

$$a' = 2a - b, \quad b' = 2b - a. \tag{1}$$

The corresponding inverse RCM transform of (1) is

$$a = \left\lceil \frac{2}{3}a' + \frac{1}{3}b' \right\rceil, \quad b = \left\lceil \frac{1}{3}a' + \frac{2}{3}b' \right\rceil, \tag{2}$$

where the symbol $\lceil \cdot \rceil$ is the ceil function. From (2), to prevent the overflow and underflow problems, the transformed pair is restricted to the value from 0 to 2^t-1. In the definition, the pixel pair (a,b) is said to be in the RCM domain (denote by $(a,b) \in \text{RCM}$) if the value of its corresponding transformed pair (a',b') meets the two constraints that $0 \le a' \le 2^t - 1$, and $0 \le b' \le 2^t - 1$.

We briefly summarize the marking steps of the RCM watermarking scheme [1] below:

Manuscript received March 5, 2008. This work was supported by the National Science Council, R.O.C., under grant NCS96-2221-E-130-010.

Yeh-Shun Chen and *Ran-Zan Wang are with the Department of Computer Science & Engineering,Yuan Ze University, Taiwan, R.O.C. (e-mail: rzwang@saturn.yzu.edu.tw).

Yeuan-Kuen Lee, Shih-Yu Huang are with the Department of Computer Science & Information Science, Ming Chuan University, Taiwan, R.O.C.

* To whom all correspondence should be addressed.

1) Divide the host image into multiple pairs of pixels.
2) For each pixel pair (*a*,*b*), conduct one of the following three marking choices:
   a) If $(a,b) \in$ RCM and their LSBs are not (1,1), transform the pair using Equation (1), set the LSB of *a*' to "1," and embed secret bit into the LSB of *b*'.
   b) If $(a,b) \in$ RCM and their LSBs are (1,1), transform the pair using Equation (1), set the LSB of *a*' to "0," and embed secret bit into the LSB of *b*'.
   c) If $(a,b) \notin$ RCM , set the LSB of *a* to "0," the original LSB bit of *a* is treated as a secret bit and embed in the image.

III. THE PROPOSED STAGANALYSIC SCHEME FOR RCM WATERMARKING

Given an image O, the pixels of the image are grouped into multiple pixel pairs, with each pair contains two pixels. According to the RCM transformation, we classify the pixel pairs of O into two types, one set is S_{RCM} and another set is $S_{\overline{RCM}}$. The set S_{RCM} consists of all of pixel pairs belonging to RCM domain, while the set of $S_{\overline{RCM}}$ contains those pixel pairs not belonging to the RCM domain.

In this subsection we examine the migration of LSB histogram of the RCM watermarking scheme [1]. Without loss of generality, let (*x*, *y*) and $(\tilde{x},\tilde{y})$ be the corresponding pixel pairs in the cover image (before the marking action) and the stego-image (after the marking action), respectively. Let us consider separately the three marking rules of RCM watermarking scheme [1] as depicted in Section II. In the first marking choice, where $(x,y) \in S_{RCM}$ and the LSB of (*x*,*y*) has one of the values in {(0, 0), (0, 1), (1, 0)}. Suppose the LSB data of the original cover image are randomly distributed, all of the three possible values mentioned above will occur in the same probability. It is easy to calculate that that the probabilities or bit 0 and bit 1 are 2/3 and 1/3, respectively. In this case, the LSB of $(\tilde{x},\tilde{y})$ is either (1, 0) or (1, 1), and each of them appears in the same probability. It is obviously that the probabilities of bit 0 and bit 1 are 1/4 and 3/4, respectively. In the second choice, where $(x,y) \in S_{RCM}$ and the LSB of (*x*, *y*) is (1, 1). The probabilities of bit 0 and bit 1 of (*x*, *y*) are 0.0 and 1.0, respectively. In this case, the LSB of $(\tilde{x},\tilde{y})$ is either (0, 0) or (0, 1), and each of them will occur in the same probability. The probabilities of bit 0 and bit 1 of $(\tilde{x},\tilde{y})$ are 3/4 and 1/4, respectively. In the third choice, where $(x,y) \in S_{\overline{RCM}}$ and the LSB of (*x*,*y*) has one of the values in {(0, 0), (0, 1), (1, 0) or (1, 1)}. In this case, the probabilities of bit 0 and bit 1 of (*x*,*y*) are 1/2 and 1/2, respectively. The same with case 2, the LSB of $(\tilde{x},\tilde{y})$ is either (0, 0) or (0, 1). The probabilities of bit 0 and bit 1 of $(\tilde{x},\tilde{y})$ are 3/4 and 1/4, respectively.

Based on above discussions, the probabilities of bit 0 and bit 1 in the LSB of the stego-image of the RCM watermarking scheme can be calculated. Assume the probability of pixel pairs belonging to RCM and the probability of pixel pairs not belonging to RCM be P_{RCM} and $P_{\overline{RCM}}$, respectively, and P_E is the embedding ratio defined by dividing the number pairs actually used to hide data by the total number of pairs of the stego-image. The probability of bit *b*={0,1} of the LSB of a stego-image can be computed using the following Eq.

$$P_{LSB}(b) = \begin{cases} P_E \times (0.375 \times P_{RCM} + 0.75 \times P_{\overline{RCM}}) + P_{\overline{E}} \times 0.5, \\ \quad if\ b = 0, \\ P_E \times (0.625 \times P_{RCM} + 0.25 \times P_{\overline{RCM}}) + P_{\overline{E}} \times 0.5, \\ \quad if\ b = 1. \end{cases} \tag{3}$$

For a natural image, assume that the LSB is randomly distributed, then the expected probability of bit 0 and the probability bit 1 are the same, i.e. $P_{LSB}(0) = P_{LSB}(1) = 0.5$. Consider the following embedding example of the RCM watermarking. Let the probability of the embeddable pairs (i.e. those pixel pairs belonging to the RCM domain) of an image be P_{RCM}=0.9, and half of the embeddable pairs are used to embed message, i.e. the embed ration P_E =0.9×0.5=0.45. From Eq. (3) we have $P_{LSB}(0)$ = 0.45×(0.375×0.9+0.75×0.1)+0.55×0.5 = 0.460625 and $P_{LSB}(1)$ = 1-0.460625 = 0.539375. We can see obvious difference of the occurrences of bit 1 and bit 0 in the LSB of the stego-image of the RCM watermarking scheme with respect to a standard natural image. Based on this observation, the following rule is designed to discriminate a stego-image of the RCM watermarking scheme from a nature image.

$$W(O) = \begin{cases} true, if\ \left|P_{LSB}(0) - P_{LSB}(1)\right| > \delta, \\ false, otherwise. \end{cases} \tag{4}$$

In Equation (4), an image is detected to be watermarked by the RCM watermarking if the measured value $\left|P_{LSB}(0) - P_{LSB}(1)\right|$ is greater than δ $(0 \le \delta \le 1)$, which is a threshold used to control the decision boundary of nature images and watermarked images. In practical implementation, the value of δ can be evaluated through the analysis of stego-images, and suitable value can be adopted to meet the requirement for specific application.

IV. EXPERIMENTAL RESULT

To show the feasibility of the proposed method, we take 500 images from content based image retrieval (CBIR) image database [11] and transform them into 8-bit gray-level format. The images are arranged in two groups, a set of 250 images used in the first test and the other set of 250 images used in the second test. The hidden messages used in our tests are produced by the pseudo random number generator.

Two experiments are conducted in this test. In the first experiment, we embed different amount of message using the RCM watermarking scheme, and measure the migration of the LSB histogram in the stego-images. Five embedding ratios 0%, 25%, 50%, 75%, and 100% are used in this test, and the obtained $\left|P_{LSB}(0) - P_{LSB}(1)\right|$ values of the stego-images are depicted in Figure1. Note that the embedding ratio here is measured with respect to the number of embeddable pairs of the cover image. From Figure 1, we can see that most of the values of $\left|P_{LSB}(0) - P_{LSB}(1)\right|$ approach zero in natural images (i.e. in the case of 0% embedding ratio), and the more data

embedded in the RCM watermarking scheme, the higher value of $|P_{LSB}(0) - P_{LSB}(1)|$ is obtained. In the second test, we measure the accuracy of the proposed method in detecting the RCM watermarking in different embedding ratio and likelihood threshold value δ. From the data shown in table 1, we see that when the likelihood threshold value δ is set 0.03, we obtain an acceptable result in detecting the RCM watermarking.

V. CONCLUSION

Most steganographic schemes, such the RCM watermarking, embed the message in the LSB of an image, because the LSB data mostly appears randomly to observers and introduces little degradations to the image. The artifacts in the LSB can still leak some statistical abnormalities, therefore gives the opportunity for steganalyzers in detecting the hidden message. This paper presents a method to break the RCM watermarking based on the observation of the bias distribution of 0 and 1 bits in the LSB of the RCM stego-images. Given the positive experimental results, we suggest that in order to increase the security of the hidden data in RCM like steganographic schemes, the alterations of the LSB histogram of an image should carefully be maintained in the data embedding process.

REFERENCES

[1] D. Coltuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Processing Lett*., vol. 14, no. 4, pp. 255–258, Apr. 2007.
[2] L. M. Marvel et. al., "Spread spectrum image steganography," *IEEE Trans. Image Process.*, vol. 8, pp. 1075–1083, 1999.
[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proc. IEEE*, vol. 87, pp. 1062–1078, 1999.
[4] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit*., vol. 37, pp. 469–474, 2004.
[5] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized LSB data embedding," *IEEE Trans. Image Process*., vol. 14, no. 2, pp. 253-266, Feb. 2005.
[6] J. Tian, "Reversible Data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video technol*., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[7] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," *IEEE Trans. Circuits Syst. Video technol*., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[8] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," *Proceedings of the ACM International Multimedia Conference and Exhibition*, pp. 27–30, 2001.
[9] 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.
[10] A. D. Ker, "Steganalysis of lsb matching in grayscale images," *IEEE Signal Processing Lett.*, vol. 12, pp. 441–444, June 2005.
[11] CBIR Image Database, University of Washington, http://www.cs.washington.edu/research/imagedatabase/groundtruth/.

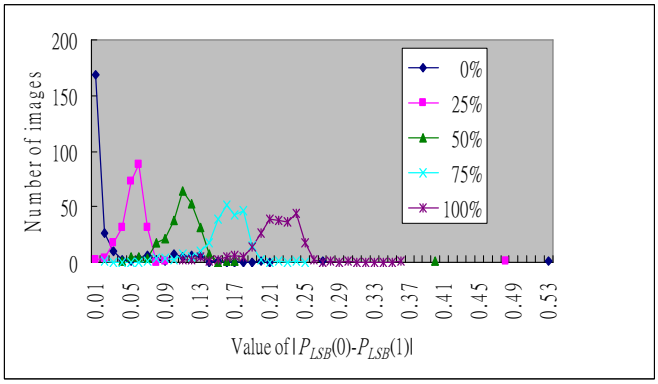

Fig. 1 The distributions of $|P_{LSB}(0) - P_{LSB}(1)|$ values of the stego-images in different embedding ratio.

Table 1. The detection accuracy of the proposed method under various embedding ratios and threshold values.

δ Embedding ratio (%)	0.01	0.02	0.03	0.04	0.05
0	60.4%	66.8%	71.2%	74.8%	77.2%
25	93.2%	84.8%	75.2%	58.4%	37.2%
50	99.6%	98.8%	95.2%	91.6%	88.8%
75	100%	100%	99.6%	99.6%	99.6%
100	100%	100%	100%	100%	100%