2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

# Revisit LSB Matching

Xiao Yi Yu[1,2,3], Aiming Wang[1]

[1]Scool of Computerv and Information Engineering，Anyang Normal University，Henan, China

[2] Scool of Information Science and Engineering， Lanzhou University， Lanzhou, China

[3] Scool of Software and Microelectronics， Peking University， Beijing, China

***Abstract*—In this paper, we propose a steganalysis algorithm to detect spatial domain least significant bit (LSB) matching steganography, which is much harder than the detection of LSB replacement. We use features based on histogram of run length and histogram characteristic function to detect the LSB Matching. Experimental results on two datasets demonstrate that this method has superior results compared with other recently proposed algorithms, and shows that the proposed method is efficient to detect the LSB matching steganography on compressed or uncompressed images.**

***Keywords- Steganography;,Steganalysis***

## I. INTRODUCTION

Steganography aims to hide the very presence of communication. That is to say, the essential goal of steganography is to conceal the presence of a hidden message. Similar to cryptanalysis, steganalysis attempts to defeat the goal of steganography. There are many techniques for stegaography. Some are simply replace the cover with the secret message. Others are quite complex using techniques such as spread spectrum or quantize index modulation etc. The most popular, frequently used and easy to implement steganographic method is the Least Significant Bit (LSB) steganography. There are two types of LSB steganography: LSB replacement and LSB matching. In LSB replacement, the least significant bit of each selected pixel is replaced by a bit from the secret message. In LSB Matching, if the bit must change, ±1 is added to the pixel value. Whether to use "+" or "−" is chosen randomly and has no effect on the hidden message. The extraction of secret message for both LSB replacement and LSB Matching work the same way: the LSB for each selected pixel is the hidden bit. LSB replacement can be uncovered relatively easily and is thoroughly examined in [1], but fewer and weaker detectors have been proposed for LSB matching.

It has been proven that the detection of LSB matching is much harder than for LSB replacement. Steganalysis methods for LSB matching are much fewer than for LSB replacement. There doses exist several detectors for LSB matching steganography in the literature. Harmsen and Pearlman [2] propose a steganalysis method using the histogram characteristic function (HCF) as a feature for distinguishing between cover and stego images. While good results were reported on a small test set using colour histograms, subsequent experiments revealed that this technique performs poorly on LSB matching in grayscale images [3]. Ker [3] extended HCF to detect LSB matching. Two novel ways of applying the HCF are: calibrating the output using a down-sampled image and computing the adjacency histogram instead of the usual histogram. Significant improvements in detection of LSB matching in grayscale images were thereby achieved. However, the experiments demonstrate it is not very efficient.

In [4], Fridrich et.al. propose a method for estimating the number of embedding changes for LSB matching steganography in images. The method uses a high-pass FIR filter and then recovers an approximate message length using a Maximum Likelihood Estimator on those stego image segments where the filtered samples can be modeled using a stationary Generalized Gaussian random process. It is shown that for images with a low noise level, such as decompressed JPEG images, this method can accurately estimate the number of embedding changes. However, this approach is not effective for never-compressed images derived from a scanner. There also exist blind techniques such as [8, 9].

Almost all these methods mentioned above have poor detection performance for LSB matching in grayscale images. In the paper, we describe a specific algorithm for the detection of LSB matching steganography. An improved method to attack the LSB matching steganography is presented. The improvements are in 2 folds. One is that we extend Ker's features to high order. The other is that we propose a new feature, the center of mass (COM) of the run length histogram, for steganalysis. With the fusion of these 2 features, our experimental results demonstrate that the proposed method is efficient to detect the LSB matching stegonagraphy using uncompressed or compressed gray scale images.

The rest of this paper is organized as follows. Section 2 reviews the previous methods on the steganalysis of LSB Matching. Section 3 proposes our new method. In Section 3, we show our experiments and compares the proposed method with the previous methods. The paper is concluded in Section 5.

## II. PREVIOUS METHODS

Ker [3] extended Harmsen's detector in two ways by applying the HCF: calibrating the output using a downsampled image and computing the adjacency histogram instead of the usual histogram. The detection procedure is described as follows:

A. calibration method:

1. Calculate the histogram $h(x)$ of the input image.

978-0-7695-4222-5/10 $26.00 © 2010 IEEE
DOI 10.1109/IIHMSP.2010.105

2. Then calculate the Discrete Fourier Transform (DFT) $H(k)$ of the histogram, which is called histogram characteristic function (HCF) in [2] and [3].

3. Calculate the center of mass (COM) of HCF:

$$C(H[k]) = \sum_{i=1}^{N/2} i\left|H[i]\right| \Big/ \sum_{i=1}^{N/2} \left|H[i]\right| \qquad (1)$$

4. Downsampling the input image by a factor of two in both dimensions using an averaging filter and calculate the COM $C'(H[k])$ of the down sampled image using (1) again.

5. Use $C(H[k])/C'(H[k])$ as a discriminator to differentiate the stego-images from the cover images.

B. adjacency histogram method:

The procedure of adjacency histogram method is very similar to the procedure of calibration method. One difference is that the histogram is defined as fallows.

$$h(x,y) = \{(i,j) | I(i,j) = x, I(i,j+1) = y\} \qquad (2)$$

where $I(i,j)$ is the pixel value at the position (i,j).

and the other difference is that the COM is calculated using

$$C(H[k,l]) = \sum_{i,j=0}^{N/2} (i+j)\left|H[i,j]\right| \Big/ \sum_{i,j=0}^{N/2} \left|H[i,j]\right| \qquad (3)$$

The COM in (1) and (3) is a kind of statistical moment of first order. Motivated by Ker's method, we extend the COM to high order as features for steganalysis. The n-th statistical moment (n-th COM) of HCF is defined as follows.

$$C_n^{DFT}(H[k]) = \sum_{i=1}^{N/2} i^n \left|H[i]\right| \Big/ \sum_{i=1}^{N/2} \left|H[i]\right| \qquad (4)$$

$$C_n^{DFT}(H[k,l]) = \sum_{i,j=0}^{N/2} (i+j)^n \left|H[i,j]\right| \Big/ \sum_{i,j=0}^{N/2} \left|H[i,j]\right| \qquad (5)$$

In [10], we proposes features called run length histogram characteristic function (RLHCF).

$$C_n^{RL}(\vec{h}) = \frac{\sum_{j=1}^{\mathrm{Max}} j^n h(j)}{\sum_{j=1}^{\mathrm{Max}} h(j)} \qquad (6)$$

where Max is the maximum run length. Let $\vec{h}_c$ be the run length histogram of the cover image and similarly $\vec{h}_s$ be the histogram of the stego image after embedding. Because of the "shrinking" effect of run length histogram after embedding, we have

$$C_n^{RL}(\vec{h}_s) < C_n^{RL}(\vec{h}_c) \qquad (7)$$

the detection algorithm as follows.

(1) For any given image, calculate $C(\vec{h})$ .

(2) Embed a random secret message with a certain length into the given image by LSB matching.

(3) Calculate $C(\vec{h}^*)$ of this new obtained image.

(4) We get the alteration rate R by using

$$R = \frac{C(\vec{h}) - C(\vec{h}^*)}{C(\vec{h})} \qquad (8)$$

(5) Normalize R to a common range [0, 1], using the following equation.

$$R = \begin{cases} 1 & R > 1 \\ R & 0 \le R \le 1 \\ 0 & R < 0 \end{cases}$$

(6) Calculate $C^2(H^2[k,l])$ , the HCF COM, of the given image using method of [3], and normalize it to [0, 1].

(7) Fusion. $F = C^2(H^2[k,l]) + R$ .

Comparing the value F with a predetermined threshold, we can determine whether the given image is a stego image.

The features of n-th COM only consider the impact of data embedding in transform domain. From our experiments, it can't improve the steganalysis performance largely. The run-length based features also have a little improved performance on LSB Matching steganalysis. We propose a new method which is also based on run-length based features in next Section.

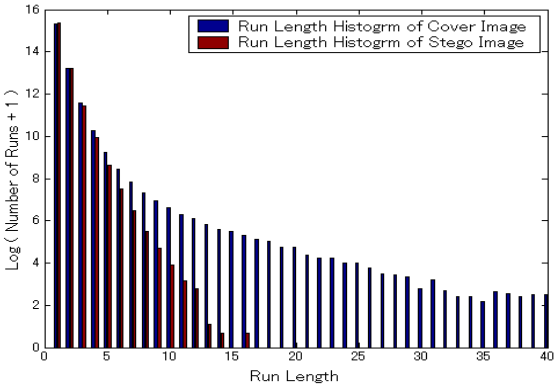


Figure 1. Run Length Histograms

## III. A NEW MTHOD

A natural image will have a lot of long runs, therefore having a run length histogram with a peak at the lowest value and a long tail as shown in the plot on the left in Fig. 1. A stego image with evidence of lots of short runs will have a run length histogram with a shorter tail and higher mid-values as shown in the plot on the right in Fig. 1. Both distributions resemble a Rayleigh distribution. This method to detect stego image was inspired by [10]. We will provide a detail analysis of the method in the context of a steganalysis problem. To apply the method to the steganalysis problem and to train a classifier, we modelled the histogram and obtained features by fitting the histogram with the generalized Rayleigh distribution. We chose this distribution because it expresses the histogram of both the stego image and the natural image observed with different parameters. Parameters are fit according to [10].

$$f(x \mid \sigma, \beta) = kxe^{-(\frac{x}{\sigma})^{\beta}} \qquad (9)$$

where $k = \frac{\beta}{\sigma^2 \Gamma(2/\beta)}$ , $\sigma = \frac{m_1 \Gamma(2/\beta)}{\Gamma(3/\beta)}$ ,

$\beta = F^{-1}(\frac{m_1^2}{m_2})$ , $m_1 = E(x)$ , $m_2 = E(x^2)$ ,

$F(x) = \frac{(\Gamma(3/\beta))^2}{\Gamma(2/\beta)\Gamma(4/\beta)}$

Using these equations, we fit the curve with the mean and variance of the histogram. Combined features in Equation (4,5,6), parameters $\sigma$ and $\beta$ are then used as features to classify the images.

## IV. EXPERIMENTAL RESULTS

Experimental results are given in this section to demonstrate the performance of our proposed method. In order to verify the proposed method, two experiments are performed here. One is carried on to test the performance of our proposed method. The second one is carried on to compare the proposed estimator performance with other estimators in the literature.

Test Image Set : 1338 Uncompressed Images. This set is downloaded from UCID [5]. All the images in UCID are high resolution uncompressed digital TIFF files with the size 512×384 or 384×512. To preserve the original statistical structure, we use 3 colour components as 3 different gray level images directly. So, totally, we have 4014 images.

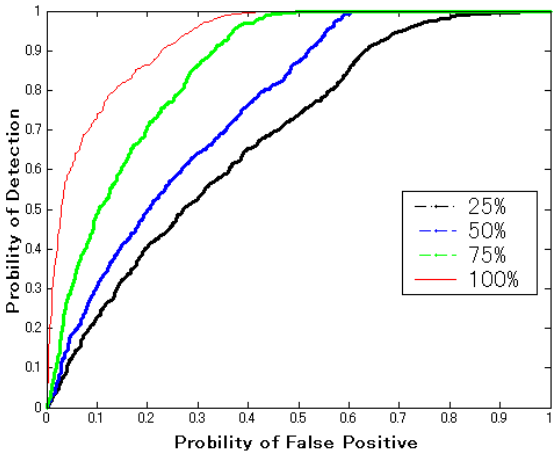


Figure 2. ROC curves

The first experiment is to test the performance of our proposed method. With embedding ratios 25%, 50%, 75% and 100%, we embed random secret message into different colour channels of images in above mentioned data sets using LSB matching data hiding method, and then detect the results by employing the proposed algorithm. Fig. 2 shows the receiver operation characteristic (ROC), where the horizontal axis represents the probability of false positive and vertical axis represents the probability of detection. The results corresponding to different stego images (the secret message length p=0.25, 0.5, 0.75, 1respectively) and different image sets are given. Fig. 2 shows results from uncompressed images set. From the experiment results, our scheme can reliably detect the presence of LSB matching steganography in both uncompressed and JPEG compressed images.

The second one is carried on to compare the proposed estimator performance with other estimators in the literature. We compare our method with Ker's two methods presented in [3] and our previous method [10]. The stego images with the secret message length p=100% are adopted in our comparison. The experimental results are shown in Fig.3 As we can see, our method outperforms Ker's methods. For images in Set I (uncompressed images), which contain a lot of noise, our method is much reliable than Ker's method. For images in Set II (compressed), images are from different sources, the noise range varies in a wide range, which make Ker's e calibrated HCF-COM method a lot of false detection. Our method also is reliable than Ker's method. We have also compared other embedding ratios, which shows our method is better than Ker's method. We don't show the results here for the limited space.

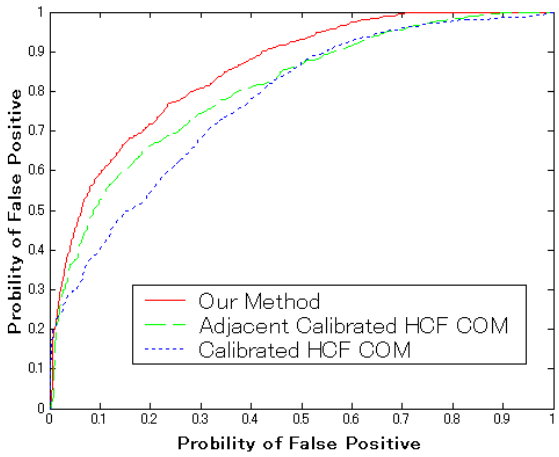


Figure 3. ROC curves Compared with Ker's Method

## V. CONCLUSIONS

We have proposed a new specific steganalysis for LSB Matching stegangoraphy. Our experiments are mainly based on the gray level run length based features and the extended Ker's features. Experimental results show it a reliable way to characterize the presence of LSB Matching steganography statistically. It is apparent, the improved techniques will also detect other kinds of steganography, and these run length based features and extended Ker's features can be used in conjunction with more sophisticated pattern classification techniques for blind steganalysis.

## ACKNOWLEDGMENT

This work was supported by Program for New Century Excellent Talents in University ( No. NCET-09-0448), the Fundamental Research Funds for the Central Universities ( No. lzujbky-2010-87), Program for Science & Technology Innovation Talents in Universities of Henan Province ( No.

2010HASTIT017) and the National Natural Science Foundation of China(No. 61075039).

## REFERENCES

[1] X. Yu, Y. Wang and N. Babaguchi, “Isotropy Based Steganalysis of Steganography in Multiple Least Significant Bits,” SPIE:Security and Watermarking of Multimedia Contents X, 2008.

[2] J. Harmsen and W. Pearlman, “Steganalysis of additive noise modelable information hiding,” in Proceedings of SPIE, vol. 5020, January 2003, pp. 131–142.

[3] A. D. Ker, “Steganalysis of LSB matching in grayscale images,” IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441–444, June 2005.

[4] J. Fridrich, D. Soukal, and M. Goljan, “Maximum likelihood estimation of length of secret message embedded using ±k steganography in spatial domain,” in Security and Watermarking of Multimedia Contents V, ser. Proceedings of SPIE, vol. 5681, January 2005, pp. 595–606.

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

[6] Content-Based Image Retrieval Image Datbase, http:// www. cs. washington. edu/ research/ imagedatabase /groundtruth/_tars. for. download/

[7] T. Holotyak, J. Fridrich, and S. Voloshynovskiy, “Blind statistical steganalysis of additive steganography using wavelet higher order statistics,” in Proceedings of the 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, ser. LNCS, vol. 3677, September 2005, pp. 273–274.

[8] M. Goljan, J. Fridrich and T. Holotyak, “New Blind Steganalysis and its Implications, ”Proc. SPIE Electronic Imaging, Photonics West, January 2006.

[9] L. Kuncheva, J. Bezdek, and R. Duin, “Decision templates for multiple classifier fusion: an experimental comparison,” Pattern Recognition, 1999.

[10] X. Yu, N. Babaguchi, “Run length based steganalysis for LSB matching steganography,” ICME 2008: 353-356

[11] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is Physics-based Liveness Detection Truly Possible with a Single Image?", IEEE International Symposium on Circuits and Systems (ISCAS), May 2010.