http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (8): 1281-1286, 2009
ISSN 1812-5638

Steganalysis Based on Difference Statistics for LSB Matching Steganography

[1,2]Jiaohua Qin, [1]Xingming Sun, [1,2]Xuyu Xiang and [1]Zhihua Xia
[1]School of Computer and Communication, Hunan University, Changsha, 410082, China
[2]Department of Mathematics and Computer, Hunan City University, Yiyang, 413000, China

Abstract: In this study, a new steganalytic method, which exploits the difference statistics of neighboring pixels, is proposed to detect the presence of spatial LSB matching steganography. In the proposed method, the differences between the neighboring pixels (DNPs), the differences between the local extrema (DLENs) and their neighbors in grayscale histogram are used as distinguishing features and the SVM is adopted to construct classifier. Experimental results show that the proposed method is efficient to detect the LSB matching steganography for the compressed and uncompressed images and outperforms other recently proposed algorithms.

Key words: Alteration rate, LSB matching, neighboring pixels, steganalysis, steganography

INTRODUCTION

The goal of steganography is to hide the very presence of communication by embedding messages into innocuous-looking cover objects (Fridrich *et al*., 2005). The most popular, frequently used and easy to implement steganographic method is the Least Significant Bit (LSB) steganography. The LSB steganographic methods can be classified into the following two categories: LSB replacement and LSB matching (also named plus/minus one embedding) (Jarno, 2006). The LSB replacement method works by replacing the least significant bits of the randomly selected pixels with the secret message bits. In LSB replacement, the even pixel values are either unmodified or increased by one, while odd ones are either decreased by one or left unchanged. This imbalance in the embedding distortion was recently utilized to detect secret messages. There is now substantial literature on LSB replacement such as (Fridrich *et al*., 2001; Dumitrescu *et al*., 2003; Ker, 2004a, b) describing sensitive statistical methods for its reliable detection.

Although, the LSB matching, a counterpart of LSB replacement, retains the favourable characteristics of LSB replacement, it is more difficult to detect from statistical perspective. In LSB matching, if the bit must change, the operation of ±1 is applied to the pixel value. The use of + or − is chosen randomly and has no effect on the hidden message. This seemingly innocent modification of the LSB embedding is significantly harder to detect, because the pixel values are no longer paired. Theoretical analysis and practical experiments show that steganalysis of LSB matching is more difficult than that of LSB replacing (Ker, 2005). As a result, none of the existing attack methods on LSB replacement can be adapted to attack LSB matching. And that, fewer and weaker detectors have been proposed for LSB matching steganography.

Harmsen and Pearlman (2003) proposed a steganalysis method using the Histogram Characteristic Function (HCF) as a feature to distinguish the cover and stego images. This method is efficient in detecting the LSB replacement for RGB color bitmaps, but ineffective in detecting the LSB matching for grayscale images. Ker (2005) extended Harmsen's method by two novel ways:

- Calibrating the output center of mass (COM) using a down sampled image
- Computing the adjacency histogram instead of the usual histogram

Significant improvements in detection of LSB matching in grayscale images were thereby achieved. Yu and Babaguchi (2008) also extended HCF and used the fusion of the COM of the run-length HCF and Ker's two-dimensional adjacency histogram to detect the LSB Matching. Zhang *et al*. (2007) proposed a method for steganalysis of LSB Matching in images with high-frequency noise. This method has superior results only when the images contain high-frequency noise, e.g., uncompressed imagery such as high-resolution scans of

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, No. 252, Lushan South Road, Yuelu District, Changsha, 410082, China Tel: 86-731-88821341 Fax: 86-731-88821341

photographs and video. However, the method is inferior to the prior art when applied to decompressed images with little or no high-frequency noise. Fridrich *et al.* (2005) proposed a maximum likelihood estimator for estimating the number of embedding changes for non-adaptive ±K embedding in images. However, they observe that this approach is not effective for never-compressed images derived from a scanner. There also exist blind techniques such as (Holotyak *et al.*, 2005; Goljan *et al.*, 2006; Lyu and Farid, 2004), which are some what effective, but they have poor detection performance for LSB matching in grayscale images.

As we can see, though some methods have been presented, the detection of LSB matching algorithm remains unresolved, especially for the uncompressed grayscale images.

In this study, we proposed a novel steganalysis method based on the statistic of DNPs and DLENs. Firstly, we calculate the sum of the DNPs with the value of zero and the DNPs with the value larger than 1. Secondly, the sums of the DLENs for local maximums and minimums in grayscale histogram are calculated. Thirdly, a stego version is built by embedding the pending image with a certain embedding length by using LSB matching steganography. Lastly, we calculate the alteration rates of DNPs and DLENs before and after LSB matching steganography and then take the alteration rates and the characteristics of DNPs and DLENs as the classifier features. Lots of experiments are done in the compressed and uncompressed images. The experimental results demonstrate that the proposed method can achieve reliable detection on LSB matching steganography.

THE PROPOSED APPROACH

There are correlations among image pixels and pixels difference. The process of LSB matching steganography disturbs the correlations of the image pixels and also the statistical distribution of the pixel differences. If we can obtain some statistical features from the statistical distribution of the pixel differences, which can denote the pixels correlations and take them as distinguishing features for LSB matching steganography in grayscale images.

As a matter of fact, pixel differences are calculated from position neighborhood and grayscale value neighborhood, respectively. And we took them as features for classifier. Good performance can be got by using these two kinds of features.

Features extraction and analysis

The DNPs features: Through the statistic analysis of DNPs on many images, it can be found that the features of DNPs can reveal the correlation between neighborhood pixels better and as a result, it is a good statistical feature to reveal the fact of message embedding.

Firstly, we define the difference histograms of images on horizontal, vertical, 45 and 135 degree, respectively diagonal as follows:

$$H_1(d) = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-2}\delta(|p_{i,j} - p_{i,j+1}|, d)}{M \times (N-1)} \quad (1)$$

$$H_2(d) = \frac{\sum_{i=0}^{M-2}\sum_{j=0}^{N-1}\delta(|p_{i,j} - p_{i+1,j}|, d)}{(M-1) \times N} \quad (2)$$

$$H_3(d) = \frac{\sum_{i=0}^{M-2}\sum_{j=0}^{N-2}\delta(|p_{i,j} - p_{i+1,j+1}|, d)}{(M-1) \times (N-1)} \quad (3)$$

$$H_4(d) = \frac{\sum_{i=1}^{M-1}\sum_{j=0}^{N-2}\delta(|p_{i,j} - p_{i-1,j+1}|, d)}{(M-1) \times (N-1)} \quad (4)$$

where, $\delta(p, q)$ if $p = q$ and 0 otherwise.

For every direction, we denote the DNPs with the value of d as $H_i(d)$, where $i = 1, 2, 3, 4$ means the direction of horizontal, vertical, 45 and 135 degree diagonal.

The sums of DNPs with the value of zero and that with the value larger than one are denoted as F_1 and F_2, respectively.

$$F_1 = \sum_{i=1}^{4} H_i(0) \quad (5)$$

$$F_2 = \sum_{i=1}^{4}\sum_{d=2}^{d_{max}} H_i(d) \quad (6)$$

where, d_{max} is the maximum difference of neighboring pixels.

After embedding a random secret message with a certain length into the given image by LSB matching, the sums of DNPs with the value of zero and that with the value larger than one are denoted as F_1^* and F_2^*, respectively.

Since, the correlations of natural images between pixels and their neighbors are very strong, the probability of DNPs with the value of zero is more in cover images than in stego images. Contrarily, the probability of DNPs with the value larger than one is less in cover images than in stego images.

We calculate the sums of DNPs before and after LSB matching for 5352 uncompressed images and 10408 converted grayscale images which are JPEG compressed.

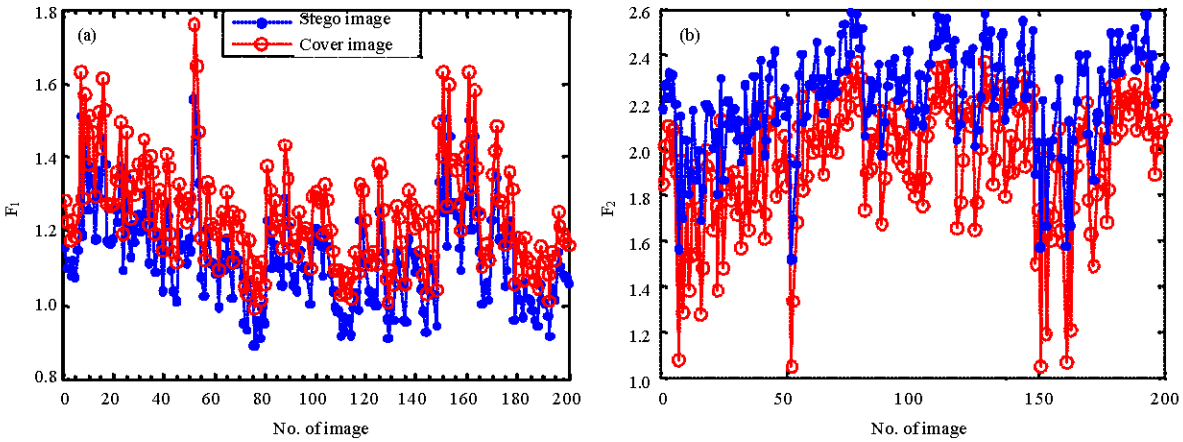

Fig. 1: The statistics of the DNPs, (a) the DNPs with the value of zero and (b) the DNPs with the value larger than one

We find that the statistical results are same with analytic conclusions. Figure 1a and b are the statistical results of the numbers of F_1 and F_2 for 200 randomly selected uncompressed grayscale images. From the Fig. 1, we can see that F_1 is greater than F_1^*, but conversely $F_2 < F_2^*$. Therefore, we can use F_1 and F_2 as features to distinguish cover images from stego images. From the Fig. 1a and b, we also can see that there is a high correlation between neighboring pixels of cover images.

The LSB matching steganography randomly changes the image pixels by ±1, moreover, the probability of DNPs with the value of zero and that of the DNPs with the value larger than one can reveal the probability of DNPs with the value of one. So, we don't make the statistical analysis on DNPs with the value of one.

The DLENs features: Let $p_{i,j}$ denote the (i, j)-th pixel value of an image. Then the unitary histogram is defined as:

$$h(x) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\delta(p_{i,j}, x)}{M \times N} \quad (7)$$

where, x is the pixel value and $0 \le x \le 255$.

The process of LSB matching can be taken as making weighed smoothness to the cover image histogram and the histogram of stego image is smoother than that of the cover image 0. This process can affect the statistical distribution of local extremum of histogram. We define the local extremum of histogram x* as follows:

$$\left(h(x^*) - h(x^* - 1)\right)\left(h(x^*) - (h(x^* + 1)\right) > 0 \quad (8)$$

Let $h_c(x)$ denote the histogram of a cover image and $h_s(x)$ denote the histogram of a stego-image. Assuming that the embedding locations are uniformly distributed and independent of the pixel values, there is a relationship between the histogram of cover image and of stego image.

$$h_s(x) \approx (1 - \tfrac{p}{2})h_c(x) + \tfrac{p}{4}(h_c(x-1) + h_c(x+1)) \quad (9)$$

By Eq. 8 and 9, for any point of local maximum x^*_{max} in cover image, there is the following relationship between the value of local maximum x^*_{max} for cover image and the value of histogram in x^*_{max} for stego-image:

$$h_s(x^*_{max}) - h_c(x^*_{max}) \approx -\tfrac{p}{4}\left(2h_c(x^*_{max}) - h_c(x^*_{max} - 1) - h_c(x^*_{max} + 1)\right) \le 0 \quad (10)$$

Similarly, for any point of local minimum x^*_{min} in a cover image, we have,

$$h_s(x^*_{min}) - h_c(x^*_{min}) \approx -\tfrac{p}{4}\left(2h_c(x^*_{min}) - h_c(x^*_{min} - 1) - h_c(x^*_{min} + 1)\right) \ge 0 \quad (11)$$

It is worth noting that x^*_{max} and x^*_{min} is the points of the local maximum and local minimum in a cover image rather than of local extremum in a stego-image. The attenuation of the local extrema by LSB matching motivated us to consider the sum of absolute differences between each local extremum and its neighbors in the histogram.

We denote the sum of the absolute differences between the local maximums and their neighbours in a cover image histogram as S_{max}.

$$S_{max} = \sum_{x^*_{max} \in h_c} |2h_c(x^*_{max}) - h_c(x^*_{max} - 1) - h_c(x^*_{max} + 1)| \quad (12)$$

The sum of the absolute differences between $h_s(x^*_{max})$ and their neighbours is given by:

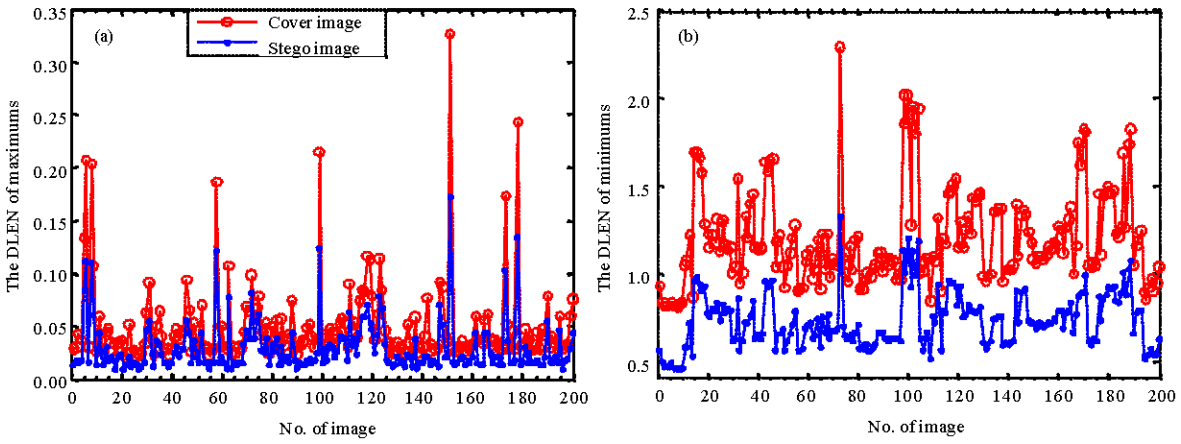

Fig. 2: The statistics of the DLENs, (a) the DLENs for maximums and (b) the DLENs for minimums

$$S^*_{max} = \sum_{x^*_{max} \in h_s} |2h_s(x^*_{max}) - h_s(x^*_{max} - 1) - h_s(x^*_{max} + 1)| \quad (13)$$

Similarly, we denote the sum of absolute differences between the local minimums and their neighbours in a cover image histogram as S_{min} and denote the absolute differences between $h_s(x^*_{min})$ and their neighbours as S^*_{min}.

Equation 10 and 11 show that the stego-images by LSB matching steganography are more smoother than the cover images,and the DLENs are lessening. Thus, $S^*_{max} < S_{max}$ and $S^*_{min} < S_{min}$.

By calculating the sums of absolute DLENs before and after LSB matching for 5352 uncompressed images and 10408 JPEG converted grayscale images, we found that the statistical results are the same with analytic conclusions. Figure 2a and b show the statistical results of the DLENs for 200 randomly selected uncompressed grayscale images. From the Fig. 2, we can also see that S_{max} is greater than S^*_{max} and S_{min} is great than S^*_{min}. Therefore, the DLENs of maximums and minimums can be used as features to distinguish the cover images from the stego images.

For the sake of convenience, let $F_3 = S_{max}$, $F_4 = S_{min}$, $F^*_3 = S^*_{max}$ and $F^*_4 = S^*_{min}$.

The change rate of the feature F_i before and after LSB matching steganography is denoted as:

$$R_i = \frac{F_i - F^*_i}{F_i} \quad (14)$$

We use these change rates as features for classifier and let $F_{i+4} = R_i$, i = 1, 2, 3, 4.

Classifier: In this study, we choose Support Vector Machine (SVM) with Gaussian kernel as classifier in our experiments because of its efficient classification performance for large scale learning. Before applying the classifier, all features are scaled (Wang and Moulin, 2007). For any training or test image, feature F_i is extracted and scaled as:

$$\tilde{F}_i = \frac{F_i - F_{i\,min}}{F_{i\,max} - F_{i\,min}}, \quad i = 1, 2, \cdots, 8 \quad (15)$$

where, F_{imax} and F_{imin} are the maximum and minimum values in F_i, respectively.

EXPERIMENT RESULTS

Here, experimental results are shown to demonstrate the performance of the proposed method. Comparative experiments are also presented to show the superiority of the method over the previous methods in terms of detection accuracy. All experimental results are reported on two sets of images.

Image datasets

Set A: 1338 uncompressed images: This image set was downloaded from UCID at http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html. All images in UCID are uncompressed digital TIFF files of 512×384 or 384×512 size with high resolution. To preserve the original statistical structure, we use 3 color components and their average as 4 different grayscale images directly. Totally, we have 5352 images.

Set B: 10408 JPEG images: This image set was downloaded from www.freefoto.com. All images are stored in JPEGs with quality factor of 75 of 600×400 or 400×600 size. They were converted to grayscale before use.

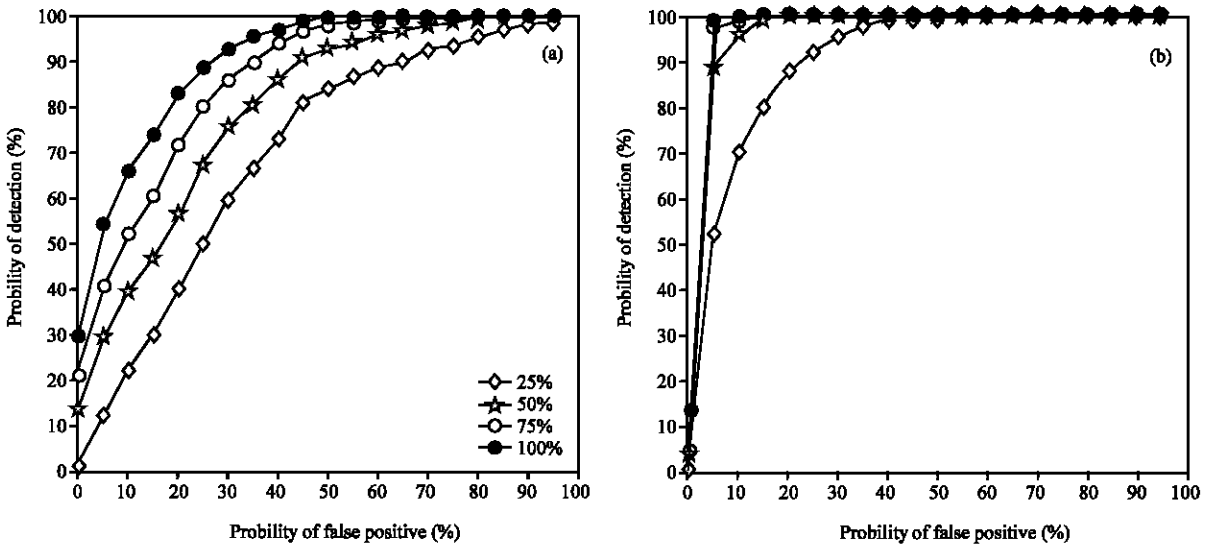

Fig. 3: ROC curves from different images, (a) the uncompressed images and (b) the compressed images

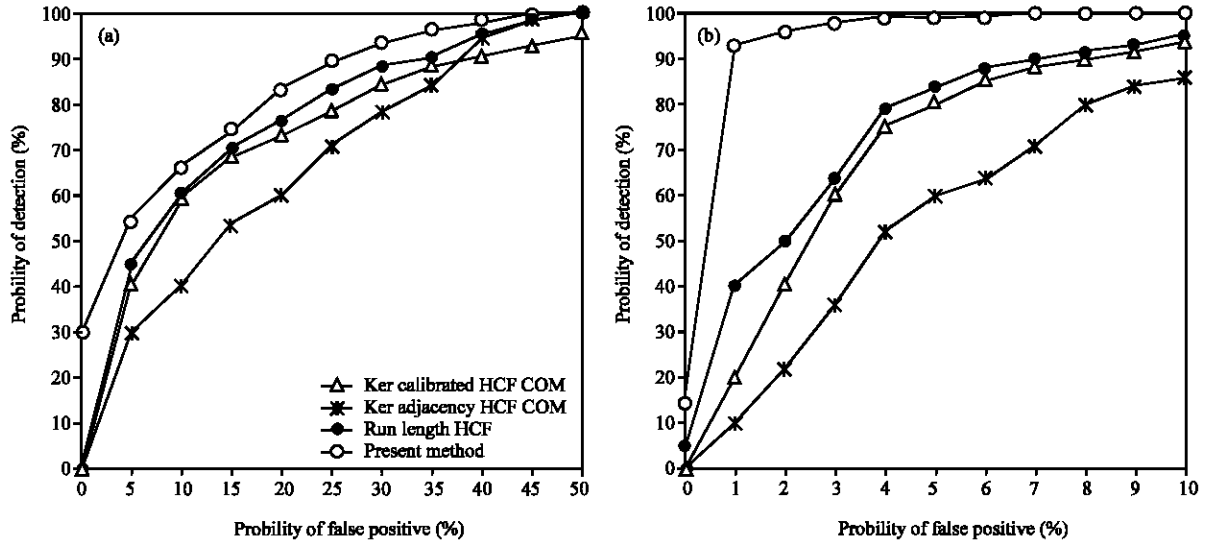

Fig. 4: ROC curves compared with Ker's and XiaoyiYu's methods for different images. (a) The uncompressed images and (b) the compressed images

Detection performance: To show the performance of our proposed method, we first produce the stego-images by embedding random secret message into all images with embedding ratios 25, 50, 75 and 100% using LSB matching steganography. We randomly select 40% original images and their corresponding stego-images for training,and the rest images are used for testing. The Receiver Operation Characteristic (ROC) curves for the uncompressed and compressed images are shown in Fig. 3a and b, where the four different curves from the top to the bottom stands for the message embedding rates of 100, 75, 50 and 25%, respectively.

From the experimental results, we can see that the detection results can reach 100% for a high embedding rate. This agrees well with the general rule. This is because the high embedding rate breaks the statistical characteristic of the image. Moreover, for the uncompressed and compressed images, the proposed method can also obtain good detection results for the low embedding and low false positive. Experimental

results showed our method gets efficiency to LSB matching steganalysis.

Comparison with existing methods: We compare our method with Ker's two detection method and Yu's RunLength method. By using the images with an embedding rate of 100%, comparison experiments are conducted on set A and set B. In Fig. 4a and b, we give Receiver Operating Characteristic (ROC) curves, for the two sets of cover images embedded with maximal-length random messages. For the uncompressed images set A, we set the false positive as 0-50%. The ROC curves are showed in Fig. 4a.

For the compressed images set B, we set the false positive as 0-10%. The ROC curves are showed in Fig. 4b.

As we all know, for the low false positive of the uncompressed images, the detection accuracies of existing methods are not ideal. From Fig. 4, it is easy to see that the proposed method achieves higher detection accuracy than the previous methods do. And both for the compressed images and the uncompressed images, this method can obtain better performance. The experimental results show that difference statistics feature is a better way to make steganalysis on LSB matching steganography.

CONCLUSION

Based on the statistical model of pixels, we in this study have proposed a new method for detection of LSB matching steganography. The ideal secure steganographic system is designed to keep the statistical distribution of cover and message unchanged. LSB matching steganographic method can approximately keep the histogram unchanged, but it cannot ensure that the statistical distributions of DNPs and DLENs are not changed. From this point, we can see that LSB matching steganography is not an ideal security. Also, for most spatial domain steganographic system, it cannot ensure to not to change the difference distribution as well. Thus, our method can also be used to detect the steganography in the spatial domain.

ACKNOWLEDGMENTS

This study is supported by Hunan Provincial National Natural Science Foundation of China (Grant No. 09JJ4033), Scientific Research Fund of Hunan Provincial Education Department (Grant No. 09B019), National Basic Research Program 973 (Grant No. 2006CB303000 and 2009CB326202), National Natural Science Foundation of China (Grant No. 60736016, 60973113 and 60973128) and Science and Technology Program of Hunan Province (Grant No. 2008FJ4221).

REFERENCES

Dumitrescu, S., X.L. Wu and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. IEEE Trans. Signal Process., 51: 1995-2007.

Fridrich, J., M. Goljan and R. Du, 2001. Detecting LSB steganography in color and gray-scale images. Multimedia IEEE, 8: 22-28.

Fridrich, J., D. Soukal and M. Goljan, 2005. Maximum likelihood estimation of length of secret message embedded using ±K steganography in spatial domain. Proc. SPIE, 5681: 595-606.

Goljan, M., J. Fridrich and T. Holotyak, 2006. New blind steganalysis and its implications. Proc. SPIE, 6072: 607201-607201.

Harmsen, J. and W. Pearlman, 2003. Steganalysis of additive noise modelable information hiding. Proc. SPIE, 5022: 131-142.

Holotyak, T., J. Fridrich and S. Voloshynovskiy, 2005. Blind statistical steganalysis of additive steganography using wavelet higher order statistics. Proceedings of the 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Sept. 19-21, Salzburg, Austria, pp: 273-274.

Jarno, M., 2006. LSB matching revisited. IEEE Signal Process. Lett., 13: 285-287.

Ker, A., 2004a. Improved detection of LSB steganography in grayscale images. Lecture Notes Comput. Sci., 3200: 97-115.

Ker, A., 2004b. Quantitative evaluation of pairs and RS steganalysis. Proc. SPIE, 5306: 83-97.

Ker, A., 2005. Steganalysis of LSB matching in grayscale images. IEEE Signal Process. Lett., 12: 441-444.

Lyu, S. and H. Farid, 2004. Steganalysis using color wavelet statistics and oneclass vector support machines. Proc. SPIE, 5306: 35-45.

Wang, Y. and P. Moulin, 2007. Optimized feature extraction for learning-based image steganalysis. IEEE Trans. Inform. Forensics Security, 2: 31-45.

Yu, X.Y. and N. Babaguchi, 2008. Run length based steganalysis for LSB matching steganography. Proceedings of the IEEE International Conference on Multimedia and Expo, Jun. 23-Apr. 26, Hannover, Germany, pp: 353-356.

Zhang, J., I.J. Cox and G. Doërr, 2007. Steganalysis for LSB matching in images with high-frequency noise. Proceedings of the IEEE 9th Workshop on Multimedia Signal Processing, Oct. 1-3, Piscataway, New Jersey, USA., pp: 385-392.