Detection of LSB Matching Revisited Using Pixel Difference Feature

Wenxiang Li[1], Tao Zhang[1], Zhenhao Zhu[1], Yan Zhang[2] and Xin Ping[2]
[1] Zhengzhou Information Science and Technology Institute
Zhengzhou, Henan 450002 - P. R. China
[e-mail: ericliwenxiang@163.com]
[e-mail: dr.zhangtao@gmail.com]
[e-mail: 19880213zhenghao@sina.com]
[2] Zhengzhou University of Light Industry
Zhengzhou, Henan 450002 - P. R. China
[e-mail: yanzhang.u@gmail.com]
[e-mail: pingxin@zzuli.edu.cn]

Received October 12, 2012; revised January 22, 2013; accepted October 24, 2013; published October 29, 2013

Abstract

This paper presents a detection method for least significant bit matching revisited (LSBMR) steganography. Previous research shows that the adjacent pixels of natural images are highly correlated and the value 0 appears most frequently in pixel difference. Considering that the message embedding process of LSBMR steganography has a weighted-smoothing effect on the distribution of pixel difference, the frequency of the occurrence of value 0 in pixel difference changes most significantly whereas other values approximately remain unchanged during message embedding. By analyzing the effect of LSBMR steganography on pixel difference distribution, an equation is deduced to estimate the frequency of difference value 0 using the frequencies of difference values 1 and 2. The sum of the ratio of the estimated value to the actual value as well as the ratio of the frequency of difference value 1 to difference value 0 is used as the steganalytic detector. Experimental results show that the proposed method can effectively detect LSBMR steganography and can outperform previous proposed methods.

Keywords: Steganography, steganalysis, LSB matching revisited, pixel difference

This work was supported by the National Natural Science Foundation of China under grant No. 60903221 and No.61272490.

http://dx.doi.org/10.3837/tiis.2013.10.011

1. Introduction

Steganography, the art of covert communication, aims at embedding secret message in innocuous cover objects (such as images and videos) so as not to arouse suspicion. By contrast, steganalysis, the counter problem of steganography, is intent on identifying the existence of secret message in a given medium.

All multimedia files, such as digital images, audios, videos, texts and documents, could be theoretically be used as the cover object of steganography. However, among all multimedia formats, digital images are the most widely used and the easiest to process. Thus, image steganography and image steganalysis are areas of great interest.

Spatial-domain least significant bit replacement (LSBR) is one of the most classical steganographic methods for images. LSBR uses a secret bit to replace the LSB of each selected pixel directly. Although LSBR steganography has good visual imperceptibility, it brings "pairs of values" to the histogram of image intensity. Based on this abnormal phenomenon, various steganalytic methods that can effectively detect the existence of secret message while accurately estimating the embedding rates have been proposed [1][2][3]. A trivial modification of LSBR is LSB matching (LSBM) steganography [4], in which the LSB of each selected pixel is compared with its corresponding secret message bit, and 1 is randomly added to or subtracted from the selected pixel value if the LSB is not equal to the message bit. For both LSBR and LSBM steganography, when the embedding rate is 100%, each selected pixel carries one bit of secret message , such that half pixel values will change. Therefore, the expected number of modifications per pixel of both LSBR and LSBM steganography is 0.5.

Unlike LSBR and LSBM, which use every single pixel as the embedding unit independently, the LSB matching revisited (LSBMR) steganography proposed by Mielikainen uses two adjacent pixels as an embedding unit, in which the first pixel carries one bit of secret message, whereas the relationship of the two pixels carries another bit [5]. In this way, the expected number of modifications per pixel can be reduced from 0.5 to 0.375 at embedding rate of 100%. This paper focuses on the detection of LSBMR steganography.

The remainder of this paper is organized as follows: Section 2 reviews previous work on the steganalysis of LSBMR steganography. In Section 3, the effect of LSBMR steganography on pixel difference distribution is analyzed, based on which, the proposed steganalytic method is introduced. Experimental results and analysis are discussed in Section 4. The conclusion and directions for future work are given in Section 5.

2. Related Work

Existing steganalytic methods can be classified into two categories: special (targeted) and universal (blind). Special steganalytic methods identify the existence of secret message by identifying the irregular statistical patterns introduced by steganographic methods, whereas universal steganalytic methods consider steganalysis as a statistical classification of cover-images and stego-images.

Tan proposed a targeted steganalytic method of LSBMR steganography using B-spline functions [6]. The author pointed out that in each pixel unit (x_i, x_{i+1}), the probability that the second pixel x_{i+1} got modified was half of the probability that the first pixel x_i got modified.

Based on this statistical imbalance, the author divided the serial of embedding units $\{(x_i, x_{i+1})\}$ into two non-intersect sub-serial $\{x_i\}$ and $\{x_{i+1}\}$ and then estimated the power of stegnoise of $\{x_i\}$ and $\{x_{i+1}\}$ using B-spline functions. The ratio of the estimated power of stegnoise of $\{x_i\}$ to that of $\{x_{i+1}\}$ was used as the steganalytic detector. Experimental results show that this approach can effectively detect LSBMR steganography. However, in practice, steganalyzers cannot have prior knowledge of the sub-serial of $\{x_i\}$ and $\{x_{i+1}\}$. Thus, this method cannot be used to detect LSBMR steganography.

The targeted methods of LSBM steganography are also useful for detecting LSBMR based on our experiments. In [7], Harmsen et al. proposed to use the center of mass of the histogram characteristic function (HCF-COM) to detect LSBM steganography. Ker improved Harmsen et al.'s work by incorporating the calibration technique with HCF-COM [8]. Li et al. further studied the calibration technique and suggested that the calibrated HCF-COM should be calculated on the difference image [9]. The experimental results show that Li's detector outperforms Ker's. On the other hand, based on the fact that the local maxima of intensity histogram would decrease whereas the local minima would increase after LSBM embedding, Zhang et al. proposed a targeted method, named local extreme method, using the sum of absolute differences between local extreme and their neighbors in intensity histogram as the detector [10]. In [11] and [12], Zhang et al. proposed a method to estimate the frequency of the occurrence of value 0 in pixel differences from the test image based on Laplacian model and used the relative estimation error between the estimated and actual value to detect LSBM steganography. Although these methods were designed to detect LSBM steganography, they are also useful for the detection of LSBMR steganography.

Blind steganalysis is equivalent to the statistical classification of cover-images and stego-images. Therefore, the key issue is finding distinguishing features capable of classifying the two types of images. Most of the early blind detection methods for spatial-domain steganography can be used for the detection of LSBMR steganography, such as the method based on image quality metrics proposed by Avcıbaş et al.[13]. In [14] and [15], Lyu and Farid used the high-order statistics of wavelet coefficients and cross-subband prediction errors as the classifying features, which are called probability density function (PDF) moments. Shi et al.'s feature set was extracted from the characteristic function (CF) moments of wavelet coefficients of image and its prediction error image [16]. Holotyak et al. selected the high-order statistics of wavelet decomposition of stego-images as the classification characteristics [17]. Goljan et al. extracted the local variance of wavelet decomposition coefficients and the absolute central moment of the residuals as the distinguishing features [18]. Based on Lyu's and Shi et al.'s work, Wang and Moulin optimized their steganalytic features from three angles: image subband decomposition, choice of features and feature evaluation and selection [19]. Both theoretical analysis and experimental results show that Wang and Moulin's method was superior to Lyu's and Shi's. Penvý et al. presented a blind steganalytic algorithm based on Markov transition probability matrix [20]. In [21], Li et al. proposed a new blind steganalytic method which viewed the image steganalysis as a problem of texture classification. From their perspective, the stego-noise introduced by message embedding was equal to stochastic textures and those statistics that are sensitive to image textures can be used as the distinguishing features. Their features comprised PDF moments of the normalized histograms of the local linear transform (LLT) coefficients of image. Motivated by [19] and [21], Zheng et al. adopted CF moments of normalized histograms of the LLT coefficients as the classifying features [22]. In [23], images were decomposited by LLT

based on some carefully selected local linear vectors and the steganalytic features were extracted from the LLT coefficients and the co-occurrence matrix.

Although various steganalytic methods have been proposed, the detection of LSBMR steganography remains unresolved. This paper presents a targeted steganalytic method of LSBMR steganography by analyzing the effect of LSBMR on pixel difference distribution. Given that image signals are highly correlated in a local neighborhood, the value 0 appears most frequently in intensity difference between adjacent pixels. In addition, considering that the message embedding process of LSBMR steganography has a smoothing effect on the distribution of pixel difference, the frequency of occurrence of difference value 0 changes most significantly in a stego-image. An equation is deduced to estimate the frequency of value 0 in pixel difference using the frequencies of values 1 and 2. The sum of the ratio of the estimated value to the actual value as well as the ratio of the frequency of difference value 1 to difference value 0 is used as the steganalytic detector, which works well for the detection of LSBMR steganography.

3. Proposed Method

3.1 Review of LSBMR Steganography

LSBMR steganography uses two adjacent pixels as an embedding unit, such that two secret bits can be embedded into each unit. Let (x_i, x_{i+1}) represent the embedding unit, and let m_i and m_{i+1} represent the secret bits to be embedded. Suppose that the corresponding unit of the stego-image is (y_i, y_{i+1}). The data embedding process of LSBMR steganography can be performed according to the following four cases [24]:

Case 1: $\mathrm{LSB}(x_i) = m_i$ and $f(x_i, x_{i+1}) = m_{i+1}$

$$(y_i, y_{i+1}) = (x_i, x_{i+1})$$

Case 2: $\mathrm{LSB}(x_i) = m_i$ and $f(x_i, x_{i+1}) \neq m_{i+1}$

$$(y_i, y_{i+1}) = (x_i, x_{i+1} \pm 1)$$

Case 3: $\mathrm{LSB}(x_i) \neq m_i$ and $f(x_i, x_{i+1}) = m_{i+1}$

$$(y_i, y_{i+1}) = (x_i - 1, x_{i+1})$$

Case 4: $\mathrm{LSB}(x_i) \neq m_i$ and $f(x_i, x_{i+1}) \neq m_{i+1}$

$$(y_i, y_{i+1}) = (x_i + 1, x_{i+1})$$

where function f is defined as: $f(a,b) = \mathrm{LSB}(\lfloor a/2 \rfloor + b)$.

From the embedding scheme of LSBMR, we can see that at most one pixel will change in each unit during message embedding and the modification is either 1 or -1. If the embedding rate is 100%, the probability of each of the given cases is 1/4, that is, every unit has the probability of 3/4 to change. Thus, the modification rate of image pixel is 3/4×1/2=0.375 bits/pixel.

3.2 Effect of LSBMR Steganography on Pixel Difference Distribution

When the embedding rate is p, the probability of Case 1, 2, 3, and 4 is evidently $p/4$. Considering the pixel difference distribution, the pixel difference values have a probability of

$3p/8$ to increase or decrease by 1 and a probability of $1-3p/4$ to remain unchanged. Suppose that the embedding pixel unit (x_i, x_{i+1}) is along horizontal direction, considering the pixel difference in horizontal direction, we have:

$$y_i - y_{i+1} = x_i - x_{i+1} + \Delta \tag{1}$$

When the embedding rate is *p*, the probability distribution of Δ is shown in **Table 1**.

Table 1. Probability distribution of Δ

Δ	1	0	-1
Probability	$3p/8$	$1-3p/4$	$3p/8$

Let $p_c(k)$ and $p_s(k)$ denote the probability of pixel difference of cover-image and corresponding stego-image respectively. **Table 1** shows that $p_s(k)$ has the following relationship with $p_c(k)$:

$$p_s(k) = p_c(k) * \{\tfrac{3}{8}p, 1-\tfrac{3}{4}p, \tfrac{3}{8}p\} \tag{2}$$

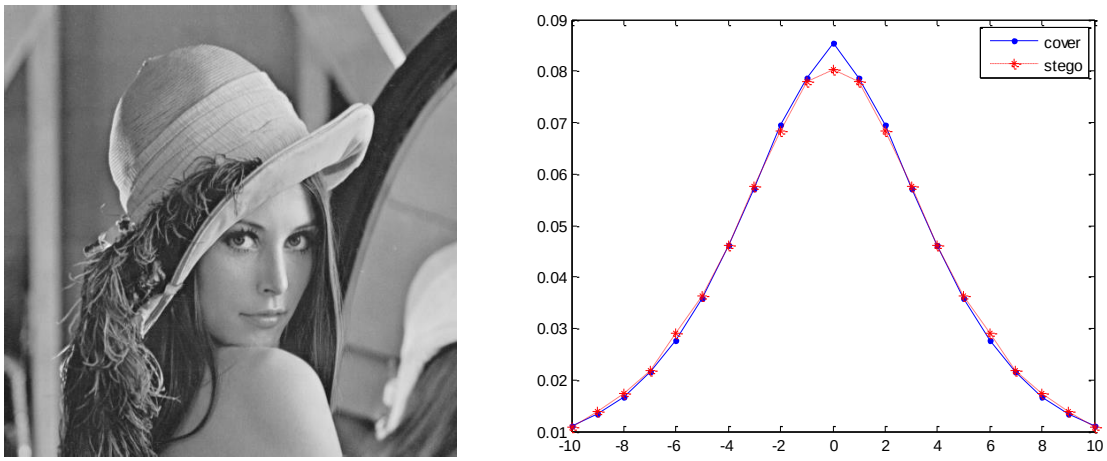
where the symbol "*" indicates sequence convolution. As indicated in Eq. (2), the message embedding procedure of LSBMR has a weighted-smoothing effect on the pixel difference distribution.

Changing the form of Eq. (2), we have:

$$\begin{aligned} p_s(k) &= \tfrac{3}{8}p \cdot p_c(k-1) + (1-\tfrac{3}{4}p)p_c(k) + \tfrac{3}{8}p \cdot p_c(k+1) \\ &= p_c(k) + \tfrac{3}{8}p\left[p_c(k-1) - 2p_c(k) + p_c(k+1)\right] \end{aligned} \tag{3}$$

From Eq. (3), we derive $p_s(0) = p_c(0) + \tfrac{3}{8}p\left[p_c(-1) - 2p_c(0) + p_c(1)\right]$. Considering that the adjacent pixels of natural images are highly correlated, the frequency of the occurrence of difference value 0 is commonly higher than that of difference value 1 and -1, i.e., $p_c(0) > p_c(1)$ and $p_c(0) > p_c(-1)$. Thus, after message embedding, the frequency of the occurrence of difference value 0 will become small, i.e., $p_s(0) < p_c(0)$. However, the modifications of the frequencies of non-zero difference values are significantly smaller than that of difference value 0 based on our experiments. Thus, we can suppose that the frequencies of non-zero difference values approximately remain unchanged during message embedding. **Fig. 1** illustrates the standard image "Lena" along with its distribution curves of pixel difference in horizontal direction. In **Fig. 1(b)**, "cover" represents cover-image while "stego" represents corresponding stego-image processed by LSBMR steganography with an embedding rate of 100%. For convenience of observation, only the range of [-10, 10] is shown. **Fig. 1(b)** shows that the frequency of difference value 0 decreases evidently, whereas the frequencies of other difference values approximately remain unchanged. Thus, we have:

$$\frac{p_s(1)}{p_s(0)} > \frac{p_c(1)}{p_c(0)} \tag{4}$$



(a) (b)

Fig. 1. Standard image "Lena" and its corresponding histograms of pixel difference distribution. (a) standard image "Lena", (b) histograms of pixel difference distribution of (a)

3.3 Proposed Steganalytic Detector

Based on the analysis in Section 3.2, if we can obtain an estimate of $p(0)$, the frequency of occurrence of the value 0 in the pixel difference of the cover-image, from the test image, the classification of cover-images and stego-images will be easier. For a stego-image with an embedded message, the estimation of $p(0)$ will be greater than the actual value, whereas for a cover-image, we expect that the estimation of $p(0)$ is close to the actual value.

For simplicity, we suppose that the frequencies of the occurrence of value 1 and 2 in pixel difference remain approximately unchanged during message embedding, that is $p_s(1) \approx p_c(1)$ and $p_s(2) \approx p_c(2)$. From Eq. (2), we obtain:

$$\begin{aligned} p_s(1) &= \tfrac{3}{8}p \cdot p_c(0) + (1-\tfrac{3}{4}p)p_c(1) + \tfrac{3}{8}p \cdot p_c(2) \\ &\approx \tfrac{3}{8}p \cdot p_c(0) + (1-\tfrac{3}{4}p)p_s(1) + \tfrac{3}{8}p \cdot p_s(2) \end{aligned} \tag{5}$$

Eq. (5) can be simplified as follows:

$$\tfrac{3}{8}p \cdot p_c(0) \approx \tfrac{3}{4}p \cdot p_s(1) - \tfrac{3}{8}p \cdot p_s(2) \tag{6}$$

Now we can obtain the estimate of the frequency of the occurrence of value 0 in pixel difference of the cover-image:

$$\hat{p}_c(0) = \frac{\tfrac{3}{4}p \cdot p_s(1) - \tfrac{3}{8}p \cdot p_s(2)}{\tfrac{3}{8}p} = 2p_s(1) - p_s(2) \tag{7}$$

Notably, the embedding rate p cannot be 0 in Eq.(7), thus, the estimating method is only suitable for stego-images. However, for cover-images, we still use Eq.(7) to estimate the frequency of difference value 0 and we hope the estimated value is close to the actual value. Since the statistical distribution of pixel difference is approximately symmetrical around 0, i.e.,

$p(x) \approx p(-x)$, $p(x)$ can be replaced by $\frac{1}{2}\left(p(x)+p(-x)\right)$.

To avoide confusion, we use $\hat{p}_s(0)$ and $\hat{p}_c(0)$ to represent the estimates of the frequency of difference value 0 from stego-image and cover-image respectively. As indicated above, the frequency of difference value 0 will decrease after message embedding. Thus, for stego-images, $\hat{p}_s(0) > p_s(0)$. However, for cover-images, we expect the estimated value to be equal to the actual value, i.e., $\hat{p}_c(0) \approx p_c(0)$. Thus, we have:

$$\frac{\hat{p}_s(0)}{p_s(0)} > \frac{\hat{p}_c(0)}{p_c(0)} \tag{8}$$

Combining Eqs.(4) and (8) yields:

$$\frac{p_s(1)}{p_s(0)} + \frac{\hat{p}_s(0)}{p_s(0)} > \frac{p_c(1)}{p_c(0)} + \frac{\hat{p}_c(0)}{p_c(0)} \tag{9}$$

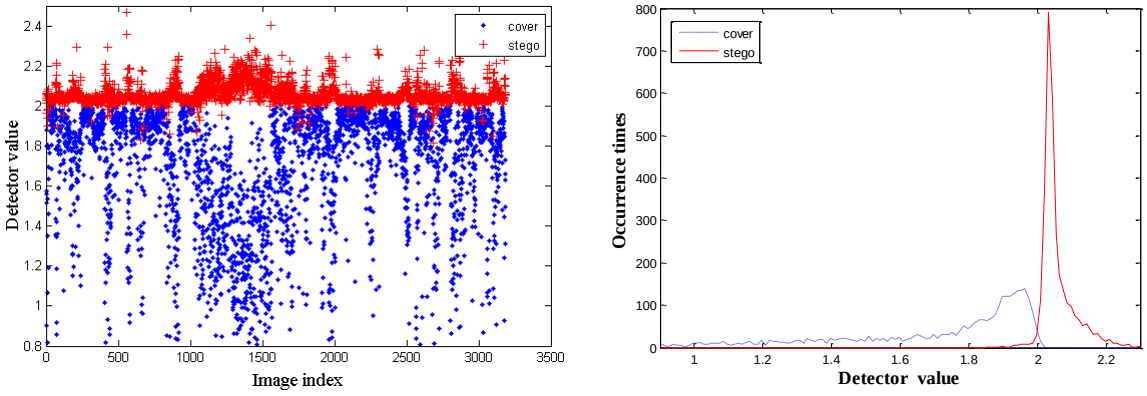
Therefore, the following feature can be selected to detect LSBMR steganography:

$$f = \frac{p(1)}{p(0)} + \frac{\hat{p}(0)}{p(0)} = \frac{3p(1)-p(2)}{p(0)} \tag{10}$$

Evidently, the detector value of stego-image f_s is greater than that of cover-image f_c:

$$f_s > f_c \tag{11}$$

Fig. 2 illustrates the detector values of cover-images and corresponding stego-images (with an embedding rate of 100%) in NRCS image database [25], where "cover" and "stego" represent cover-images and stego-images respectively. **Fig. 2** shows that a large statistical difference exists between cover-images and stego-images and that the proposed detector can effectively detect LSBMR steganography.



(a) (b)

Fig. 2. Distributions of detector values of cover-images and stego-images. (a) dotted diagram and (b) histogram

4. Experimental Results and Analysis

4.1 Image Database

In order to test the performance of the proposed detector in Eq. (10) and compare our method with previous methods, the following image databases are chosen to do the experiments:

(1) NRCS image database containing 3185 high-precision scanned color images with a fixed size of 2100×1500 or 1500×2100. We convert the color images into gray-level images before calculation [25].

(2) All images in NRCS database are down-sampled to 700×500 or 500×700. We denote this image database by "NRCS_D".

(3) BOWS image database containing 10000 uncompressed gray images with a fixed size of 512×512 [26].

4.2 Comparison with Special Steganalytic Methods

We compare our method with the local extreme method [10] and the method proposed in [11] using the three aforementioned image databases. At embedding rates of 100% and 50%, we embed messages into all images in each database using LSBMR steganography and then classify cover-images and stego-images using the proposed algorithm, the local extreme method and the method in [11]. The receiver operating characteristic (ROC) curves on the three image databases at embedding rates of 100% and 50% are shown in **Figs. 3** and **4** respectively, where "Proposed" represents the algorithm in this paper, whereas "LE" and "LM" represent the local extreme method and the method in [11], respectively.

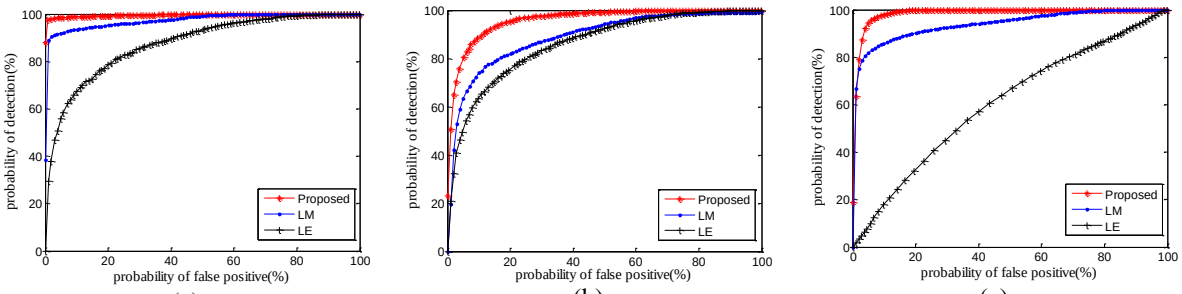


Fig. 3. ROC curves of three special methods on different image databases (at embedding rate of 100%). (a) NRCS; (b) NRCS_D; (c) BOWS

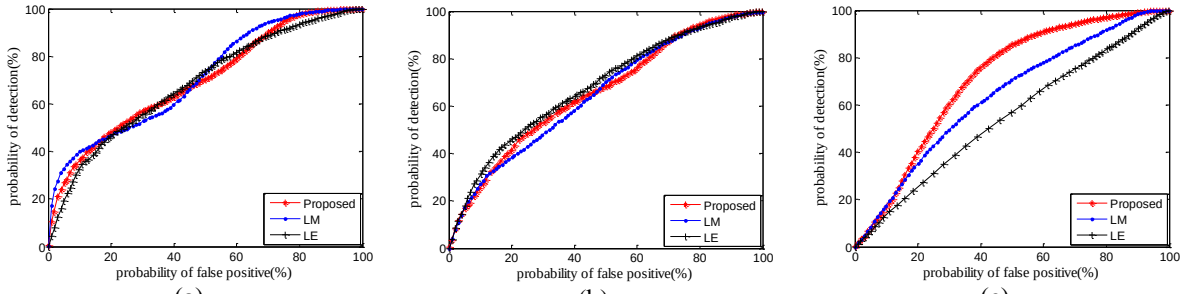


Fig. 4. ROC curves of three special methods on different image databases (at embedding rate of 50%). (a) NRCS; (b) NRCS_D; (c) BOWS

The following four indicators are used to measure the performance of the detection algorithm: (1) area under ROC curve, noted as "AUC"; (2) rate of correct detection when the false positive rate equals to the false negative rate, noted as "TP_E"; (3) the false positive rate at the true positive rate of 80%, noted as "FP_80"; and (4) the false positive rate at the true positive rate of 50%, noted as "FP_50". The closer to 1 the first two indicators are, the better the performance of the detection algorithm, and the closer to 0 the latter two indicators are, the better the performance of the detection algorithm.

The detection performance indicators on the three image databases at embedding rates of 100% and 50% are shown in **Tables 2** and **3** respectively, where "Proposed" represents the algorithm in this paper, whereas "LE" and "LM" represent local extreme method and the method in [11] respectively. The values in bold indicate the best detection performance for each instance.

Table 2. Comparison of detection performance among three special methods at embedding rate of 100%

Database	Method	AUC	TP_E	FP_80	FP_50
NRCS	Proposed	**0.9957**	**0.9802**	**0.0000**	**0.0000**
	LE	0.8750	0.7931	0.2100	0.0389
	LM	0.9740	0.9272	0.0097	0.0000
NRCS_D	Proposed	**0.9603**	**0.8951**	**0.0512**	**0.0097**
	LE	0.8609	0.7752	0.2458	0.0477
	LM	0.8877	0.8154	0.1589	0.0298
BOWS	Proposed	**0.9851**	**0.9446**	**0.0196**	**0.0099**
	LE	0.6062	0.5692	0.6882	0.3271
	LM	0.9371	0.8751	0.0395	0.0102

Table 3. Comparison of detection performance among three special methods at embedding rate of 50%

Database	Method	AUC	TP_E	FP_80	FP_50
NRCS	Proposed	0.6977	0.6135	0.6100	**0.2198**
	LE	0.6854	**0.6285**	0.5787	0.2421
	LM	**0.7102**	0.5978	**0.5513**	0.2562
NRCS_D	Proposed	0.6603	0.6122	0.6396	0.2728
	LE	**0.6824**	**0.6261**	**0.5821**	**0.2433**
	LM	0.6504	0.5931	0.6091	0.3212
BOWS	Proposed	**0.7110**	**0.6750**	**0.4392**	**0.2497**
	LE	0.5477	0.5345	0.7563	0.4248
	LM	0.6379	0.6005	0.6318	0.2982

Fig. 3 and **Table 2** show that, at the embedding rate of 100%, the proposed method can effectively detect LSBMR steganography and is clearly superior to the local extreme method and the method in [11] when applied on all the three aforementioned image databases.

Fig.4 and **Table 3** show that, at the embedding rate of 50%, the three methods exhibit almost the same performance on NRCS image databases. When applied on the NRCS_D image database, the performance of the proposed method outperforms the method in [11] but is inferior to the local extreme method. When applied on the BOWS image database, the proposed method outperforms the two other targeted steganalytic methods.

Contrasting **Fig. 3(a)** with **Fig. 3(b)** and **Fig. 4(a)** with **Fig. 4(b)**, we can see that the performance of all the three methods on NRCS image database is better than that on NRCS_D image database. The reason is that the correlation between adjacent pixels is weakened after down-sampling process, thus, minimizing the difference between cover-images and stego-images.

The local extreme method is effective in detecting LSBMR steganography on NRCS and NRCS_D image databases but is ineffective on BOWS database. A possible reason is that the local extreme method uses the sum of absolute differences between local extreme and their neighbors in intensity histogram as the detector. Thus, for images with high noises, i.e., images in NRCS and NRCS_D image databases, the method exhibits good performance. However, for images with low noises, i.e., images in BOWS image database, the method is ineffective.

4.3 Comparison with Universal Steganalytic Methods

Since the detection of LSBMR steganography on NRCS_D image database is more difficult than that on the two other image databases, we only compare our method with the following two universal steganalytic methods on this database:

(1) Optimized feature extraction for steganalysis (denoted by OPT156) [19]. Wang and Moulin extracted both PDF moments and CF moments features from wavelet and prediction error subbands. In our experiment, we set the order N to be 6 to obtain 156 dimensional features.

(2) Image textural features for steganalysis of spatial domain steganography (denoted by LLTCM120) [23]. Xiong et al. proposed a 120-dimensional feature set which extracted from the LLT coefficients histogram and cooccurrence matrix.

For ease in computation, we use Fisher linear discriminant as the classifier. Half of the images in NRCS_D database are randomly selected for training and the rest are used for testing. The following performance results of OPT156 and LLTCM120 on this database are averaged over 20 random training/testing splits in order to avoid flukes for any particular split. The result is shown in **Table 4**. The values in bold indicate the best detection performance for each instance.

Table 4. Comparison of detection performance with blind steganalytic methods on NRCS_D database

Embedding rate	Methods	AUC	TP_E	FP_80	FP_50
100%	Proposed	**0.9603**	**0.8951**	**0.0512**	**0.0097**
	OPT156	0.8940	0.8186	0.1696	0.0584
	LLTCM120	0.8350	0.7500	0.2871	0.1220
50%	Proposed	0.6603	0.6122	0.6396	0.2728
	OPT156	0.7088	0.6574	0.4947	0.2299
	LLTCM120	**0.7462**	**0.6623**	**0.4629**	**0.2138**

Table 4 shows that the performance of the proposed method is evidently superior to OPT156 and LLTCM120 at embedding rate of 100% but is inferior to OPT156 and LLTCM120 at embedding rate of 50%. However, as our method using only a single feature, it is easier to calculate and does not require classifiers. The feature dimensions of OPT156 and LLTCM120 are 156 and 120 respectively, thus resulting in high computing complexity.

5. Conclusion and Future Work

This paper analyzes the effect of LSBMR steganography on the distribution of pixel difference and estimates the frequency of occurrence of value 0 in pixel difference using the frequency of occurrence of other values. The sum of the ratio of estimated value to actual value as well as the ratio of the frequency of difference value 1 to difference value 0 is used as the steganalytic detector. Experimental results show that the proposed method can effectively detect LSBMR steganography, especially at high embedding rate. Directions for future work include the

enhancement of detection performance at low embedding rates and the establishment of an algorithm for estimating the embedding rate of LSBMR steganography.

References

[1] Jessica Fridrich, Miroslav Goljan and Rui Du, "Detecting LSB steganography in color and gray-scale images," *IEEE Multimedia*, vol.8, no. 7, pp. 22-28, October-December, 2001. Article (CrossRef Link)

[2] Sorina Dumitrescu, Xiaolin Wu, Zhe Wang, "Detection of LSB steganography via sample pair analysis," in *Proc. of the 5th Int. Workshop on Information Hiding*, *Lecture Notes in Computer Science*, vol. 2578, pp.355-372, October 7-9, 2002. Article (CrossRef Link)

[3] Tao Zhang, Xijian Ping, "A new approach to reliable detection of LSB steganography in natural images," *Signal Processing*, vol.83, no.10, pp.2085-2093, October, 2003. Article (CrossRef Link)

[4] Toby Sharp, "An implementation of key-based digital signal steganography," in *Proc. of the 4th Workshop on Information Hiding*, *Lecture Notes in Computer Science*, vol. 2137, pp.13-26, April 25-27, 2001. Article (CrossRef Link)

[5] J. Mielikainen, "LSB Matching Revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp.285-287, May, 2006. Article (CrossRef Link)

[6] Shunquan Tan, "Steganalysis of LSB matching revisited for consecutive pixels using B-spline functions," in *Proc. of International Workshop on Digital Forensics and Watermarking*, *Lecture Notes in Computer Science*, vol. 7128, pp.16－29, 2012. Article (CrossRef Link)

[7] Jeremiah J. Harmsen and William A. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Proc. of SPIE , Electronic Imaging, Security and Watermarking of Multimedia Contents V*, vol.5020, pp.131-142, January 21-24, 2003. Article (CrossRef Link)

[8] Andrew D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol.12, no.6, pp.441- 444, June, 2005. Article (CrossRef Link)

[9] Xiaolong Li, Tieyong Zeng and Bin Yang, "Detecting LSB matching by applying calibration technique for difference image," in *Proc. of 10th ACM Multimedia & Security Workshop*, pp. 133-138, September 22-23, 2008. Article (CrossRef Link)

[10] Jun Zhang, Ingemar J. Cox and Gwenaël Doërr, "Steganalysis for LSB matching in images with high-frequency noise," in *Proc. of IEEE Workshop on Multimedia Signal Processing*, pp.385-388, October 2007. Article (CrossRef Link)

[11] Tao Zhang, Wenxiang Li, Yan Zhang, Ergong Zheng and Xijian Ping. "Steganalysis of LSB matching based on statistical modeling of pixel difference distributions," *Information Sciences*, vol.180, no. 23, pp.4685-4694, December 2010. Article (CrossRef Link)

[12] Tao Zhang, Wenxiang Li, Yan Zhang and Xijian Ping, "Detection of LSB matching steganography based on the Laplacian model of pixel difference distributions," in *Proc. of IEEE 17th Int. Conf. on Image Processing*, pp.221-224, September 26-29, 2010. Article (CrossRef Link)

[13] İsmail Avcıbaş, Nasir Memon and Bülent Sankur, "Steganalysis using image quality metrics," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp.221-229, February 2003. Article (CrossRef Link)

[14] Siwei Lyu and Hany Farid, "Detecting hidden messages using higher-order statistics and support vector machines," in *Proc. of 5th International Workshop on Information Hiding*, *Lecture Notes in Computer Science*, vol. 2578, pp.340－354, 2003. Article (CrossRef Link)

[15] Siwei Lyu and Hany Farid, "Steganalysis using higher-order image statistics," *IEEE Transactions on Information and Forensics Security*, vol. 1, no. 1, pp.111－119, March 2006. Article (CrossRef Link)

[16] Yun Q. Shi, Guorong Xuan, Dekun Zou, Jianjiong Gao, Chengyun Yang, Zhenping Zhang, Peiqi Chai, Wen Chen and Chunhua Chen, "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network," in *Proc. of IEEE Int. Conf. on Multimedia and Expo, IEEE Computer Society*, vol. 1, pp.269-272, 2005. Article (CrossRef Link)

[17] Taras Holotyak, Jessica Fridrich and Sviatoslav Voloshynovskiy, "Blind statistical steganalysis of additive steganography using wavelet higher order statistics," in *Proc. of 9th IFIP Conf. on Communications and Multimedia Security*, pp.273–274, September 19-21, 2005. Article (CrossRef Link)
[18] Miroslav Goljan, Jessica Fridrich and Taras Holotyak, "New blind steganalysis and its implications," in *Proc. of SPIE Electronic Imaging*, pp.1-13, January 16-19, 2006. Article (CrossRef Link)
[19] Ying Wang and Pierre Moulin, "Optimized feature extraction for learning-based image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp.31-45, March, 2007. Article (CrossRef Link)
[20] Tomáš Pevný, Patrick Bas and Jessica Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 2, pp. 215-224, March, 2010. Article (CrossRef Link)
[21] Bin Li, Jiwu Huang and Yun Q. Shi, "Textural Features Based Universal Steganalysis," in *Proc. of Security, Forensics, Steganography and Watermarking of Multimedia Contents X, SPIE-IS & T Electrinic Imaging*, vol. 6819, no.12, pp.1-12, 2008. Article (CrossRef Link)
[22] Ergong Zheng, Xijian Ping and Tao Zhang, "Local linear transform and new features of histogram characteristic functions for steganalysis of least significant bit matching steganography," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 4, pp. 840-855, April, 2011. Article (CrossRef Link)
[23] Gang Xiong, Xijian Ping, Tao Zhang and Xiaodan Hou, "Image textural features for steganalysis of spatial domain steganography," *Journal of Electronic Imaging*, vol. 21, no. 3, pp. 033015-1-033015-15, July-September, 2012. Article (CrossRef Link)
[24] Weiqi Luo, Fangjun Huang and Jiwu Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Transactions Information Forensics and Security*, vol. 5, no. 2, pp. 201-214, June, 2010. Article (CrossRef Link)
[25] USDA NRCS Photo Gallery, 2010. http://photogallery.nrcs.usda.gov.
[26] P. Bas and T. Furon. 2007. http://bows2.gipsa-lab.inpg.fr.

Wenxiang Li received his M.S. degree in Signal and Information Processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2010, and is currently pursuing the Ph.D. degree in Zhengzhou Information Science and Technology Institute. His research interests include information hiding and image forensics.

Tao Zhang received his M.S. and Ph.D. degrees in Signal and Information Processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2000 and 2003, respectively. He is currently an Associate Professor with Department of Information Science, Zhengzhou Information Science and Technology Institute. His research interests include information hiding, image processing and pattern recognition.

Zhenhao Zhu received his B.S. degree in Electrical Information Engineering from Wuhan University of Technology, Wuhan, China, in 2010, and M.S. degree in Signal and Information Processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2013. His research interests include information hiding and image processing.

Yan Zhang received her M.S. degree in Signal and Information Processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2001. She is currently a lecturer with College of Computer and Communication Engineering, Zhengzhou University of Light Industry. Her research interests include image processing and pattern recognition.

Xin Ping received her B.S. degree in Information Science from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2007. She is currently a assistant engineer with Modern Education Technology Management Center, Zhengzhou University of Light Industry. Her research interests include computer technology and Internet information security.