2013 10th IEEE International Conference on Control and Automation (ICCA)
Hangzhou, China, June 12-14, 2013

A Special Detector for the Edge Adaptive Image Steganography Based on LSB Matching Revisited*

Zhenhao Zhu, Tao Zhang, and Baoji Wan

Abstract— **Based on the analysis of the pixel value difference (PVD) histograms of the cover and stego-images, a special steganalyzer is proposed for the edge adaptive image steganography based on least-significant-bit matching revisited (EA-LSBMR). The EA-LSBMR steganography utilizes the sharper edge regions within the cover images to embed the secret message firstly, which achieves a higher security. However, there exists unavoidable weakness: abnormal increasing at some position of the PVD histogram. The special steganslytic method is designed using the weakness of the EA-LSBMR steganography. Extensive experimental results show that the proposed method can defeat the EA-LSBMR steganography effectively.**

I. Introduction

As an important technique of information hiding, steganography has already been widely used in the field of information security. It is an art of embedding secret messages into cover-objects (such as digital images and videos), without arousing the third party's suspicion. On the other hand, Steganalysis is the set of techniques that are aimed to distinguish between cover objects and stego objects. Generally speaking, if the steganalytic algorithm can give a higher probability than random guessing to judge whether a given object is cover or not, the steganographic system is considered broken.

Spatial-domain least significant bit (LSB) embedding is the simplest and most common steganographic algorithm. LSB replacement, as its name suggests, works by replacing the LSB planes of a cover image by the message bits. In the process, the Pair of Value (PoV) artifact in the histogram of a stego image is introduced, which allows various steganalysis methods to attack LSB replacement successfully, such as χ^2 attack [1], regular/singular groups (RS) analysis [2], sample pair analysis [3] and the general framework for structural steganalysis [4].

A trivial modification of LSB replacement is LSB matching (LSBM) [5] in which one is randomly added to or subtracted from the corresponding pixel value if the message bit to be embedded does not match the LSB of the cover pixel. So the pair of value artifact in the histogram introduced by LSB replacement is avoided, and the security of LSB matching is improved. Therefore, the steganalysis methods mentioned above are ineffective in detecting the LSBM. In recent years, several steganalytic algorithms have been proposed to detect the LSBM [6]-[12]. Meanwhile, some blind steganalytic methods [13]-[16] also can be used for detecting the LSBM with relatively high detection accuracy.

In [17], Mielikainen proposed a new steganographic algorithm called LSB matching revisited (LSBMR), which used a pair of pixels as an embedding unit. For LSBMR steganography, the LSB of the first pixel in the unit carries one bit of secret message, and the relationship of the two pixels carries another bit of secret message. So it makes fewer changes to the cover image than LSBM with the same payload and is thus more difficult to detect.

In fact, all of the above-mentioned algorithms, including LSB replacement, LSBM and LSBMR, are designed without considering the relationship between the image content and the size of secret message. We know that the different regions of a cover image have different capacities for hiding the message. Obviously, the regions which have complex texture can bear more secret messages than flat regions and they are harder to classify as a result of presenting more complicated statistical features. Based on the observation above, Luo et al. [18] proposed an edge adaptive scheme and applied it to the LSBMR-based method. The scheme embeds the secret message into the sharp edge regions firstly according to a threshold determined by the size of secret message and image content, in which the cover image is divided into nonoverlapping blocks of $Bz \times Bz$ pixels in advance. Extensive experimental results show that Luo's algorithm is more secure than others, such as, LSB replacement, LSBM and LSBMR. This paper focuses on the steganalysis of EA-LSBMR.

Recently, Tan [19] pointed out that LSBMR steganography introduces intrinsic statistical imbalance in secret message embedding process and constructed a dimensionless discriminator using B-spline smoothing which can detect the LSBMR steganography successfully.

Up to now, there is no targeted steganalysis method proposed capable of detecting EA-LSBMR effectively, especially with a relative low payload. In this paper, we propose a steganalysis algorithm that exploits the fact that the PVD histogram of the image abnormally fluctuates due to the message embedding using EA-LSBMR steganography. Extensive experimental results indicate that our proposed scheme has superior performance, especially when the payload is low.

*Research supported by the National Natural Science Foundation of China (No. 60903221, 61272490).

Zhenhao Zhu is with the Zhengzhou Information Science and Technology Institute, Zhengzhou, China (phone: 86-371-81630726; e-mail: bravezzh@gmail.com).

Tao Zhang is with the Zhengzhou Information Science and Technology Institute, Zhengzhou, China (e-mail: brunda@163.com).

Baoji Wan is with the Zhengzhou Information Science and Technology Institute, Zhengzhou, China (e-mail: dirker2012@163.com).

978-1-4673-4708-2/13/$31.00 ©2013 IEEE

The rest of this paper is organized as follows. The EA-LSBMR steganography is described in Section II as well as the proposed steganalytic method for the EA-LSBMR steganography. Experimental results are shown in Section III and Section IV concludes the paper and outlines future research directions.

II. THE PROPOSED METHOD

A. *Weakness of EA-LSBMR steganography*

For the convenience of explanation, let the cover-pixel, stego-pixel and threshold be x_i , x_i' and *T*, respectively. In [18], we know that if $|x_i'-x_{i+1}'|<T$ after EA-LSBMR steganography, the pixel unit (x_i',x_{i+1}') need to be readjusted as (x_i'',x_{i+1}'') using (1):

$$\begin{aligned}(x_i'',x_{i+1}'')=\arg\min_{(e_1,e_2)}\{|e_1-x_i|+|e_2-x_{i+1}|\,|\,e_1=x_i'+4k_1,e_2\\ =x_{i+1}'+2k_2,|e_1-e_2|\ge T,0\le e_1,e_2\le 255,0\le T\le 31,k_1,k_2\in Z\}.\end{aligned} \quad (1)$$

There are two cases to readjust the embedding units after data embedding. Without loss of generality, assume that $0\le x_i<x_{i+1}\le 255$. If $d=|x_{i+1}-x_i|=T$, $d'=|x_{i+1}'-x_i'|=d-1=T-1<T$, for any x_i' and x_{i+1}' , x_i' , x_{i+1}' ∈ [0,255], we let $R_l=[0,x_i')$, $R_r=(x_{i+1}',255]$. Since $|R_l|+d+|R_r|=256$, then we get $|R_l|+|R_r|\ge 256-31=225$. Therefore, there must exist a region R_l or R_r which satisfies $|R_l|\ge 4$ or $|R_r|\ge 2$. The two ways to readjust the pixel units are listed as follows:

Case 1: If $|R_r|\ge 2$, let $x_i''=x_i'$, $x_{i+1}''=x_{i+1}'+2\le 255$ (k_1=0, k_2=0) then $d''=d'+2=T-1+2=T+1\ge T$.

Case 2: If $|R_l|\ge 4\ \&\ |R_r|<2$, let $x_i''=x_i'-4\ge 0$, $x_i''=x_{i+1}'$

(k_1=-1, k_2=0) then $d''=d'+4=T-1+4=T+3\ge T$.

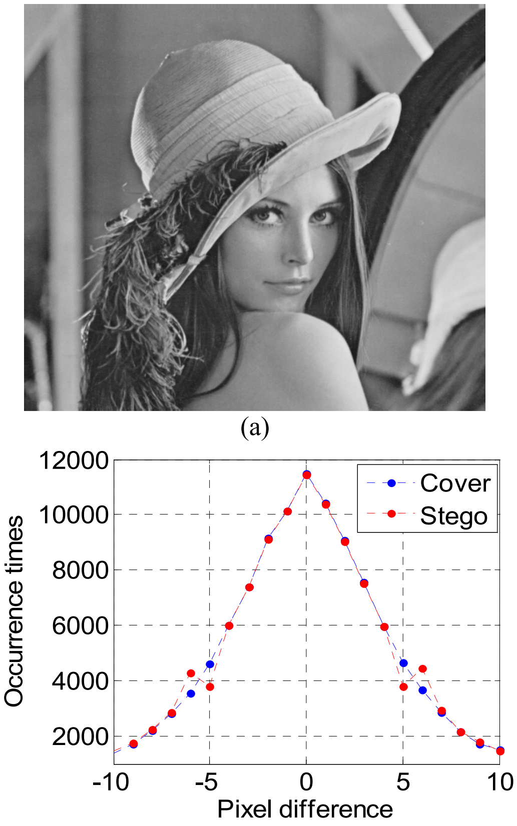
Here is an example to explain the readjusting process. Suppose the pixel embedding unit $(x_i,x_{i+1})=(58,53)$, the secret messages $m_i=1$, $m_{i+1}=1$ and the threshold $T=5$, we have $d=|x_{i+1}-x_i|=5\ge T$ and $\mathrm{LSB}(58)=0\ne m_i$, $\mathrm{LSB}\left(\left\lfloor\frac{(58-1)}{2}\right\rfloor+53\right)=1=m_{i+1}$. Then we obtain $(x_i',x_{i+1}')=(57,53)$ according to LSBMR steganography. The new difference is $d'=|57-53|=4<T$. We need to readjust the pixels according to (1) and get $k_1=0$, $k_2=-1$, namely,

$$x_i''=x_i'+4k_1=57+4\times 0=57$$

$$x_{i+1}''=x_{i+1}'+2k_2=53-2\times 1=51 .$$

It is easy to get that $d''=|57-51|=6$, $\mathrm{LSB}(57)=m_i$ and $\mathrm{LSB}\left(\left\lfloor\frac{(57-1)}{2}\right\rfloor+51\right)=m_{i+1}$. Based on the new pixels (x_i'',x_{i+1}'') , the receiver can extract the secret message correctly when *T*=5.

From the example above, it can be observed that the number of embedding units whose absolute differences equal to 5 will decrease by one and meanwhile the number of embedding units whose absolute difference equal to 6 will increase by one. It is believed that the pixel value difference (PVD) histogram of a stego-image will abnormally decrease on some position and increase on the other position as the number of readjusting embedding units increases. In order to get the minimal pixel modifications, the absolute differences of most of the embedding units become *T*+1 after readjusting. Fig. 1 depicts the PVD histograms that have obvious artifacts which are generated by EA-LSBMR steganography. The abnormally decreasing and increasing appear in the PVD histogram of the stego-image at some certain point (such as decreasing at 5 and increasing at 6 in Fig. 1 (b)).


(a)

(b)

Figure 1. The 'Lena' image and its PVD histogram after 30% embedding. (a) 'Lena' image. (b) PVD histogram of 'Lena' image after 30% embedding.

As is shown in Fig. 1, the fluctuations symmetry appearing in the PVD histogram of the stego-image are obvious, which can be utilized to design a steganalysis algorithm to reliably detect the EA-LSBMR steganography.

B. Feature extraction

Based on the fact that the value of PVD histogram abnormally fluctuates at the symmetry position, as is shown in Fig. 1 (b) , the symmetry differencing feature derived from the PVD histogram is extracted. Let the PVD histogram and the size of the image be h and M×N. Because the threshold $T \in [0,31]$, the $h(d)$, $-32 \le d \le 32$ is taken into account.

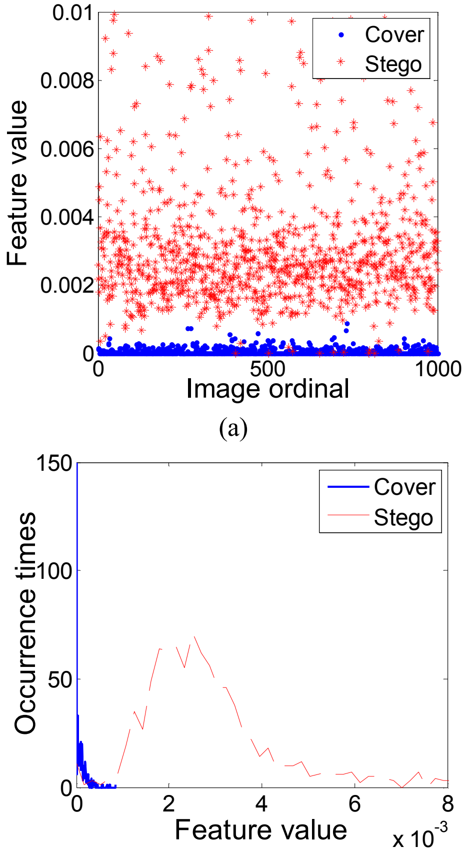
Let **M** be the set of the m which satisfies (2), then the feature D is calculated according to (3).

$$\begin{cases} h(m) < h(m-1) \\ h(m) < h(m+1) \\ h(-m) < h(-m+1) \\ h(-m) < h(-m-1). \end{cases} \tag{2}$$

where $1 \le m \le 31$.

$$D = \max\left\{ \frac{h(m+1)-h(m)+h(-m-1)-h(-m)}{M \times N} \middle| m \in \mathbf{M} \right\}. \tag{3}$$

let D=0, when there is no value satisfy (2).



(a)

(b)

Figure 2. Distributions of the features for cover and stego images over image database NRCS. (a) Dotted diagram. (b) Histogram.

Fig. 2 illustrates the distributions of the steganalytic feature values of stego-images over database NRCS [20] with the embedding rate of 20%. It can be seen that there is a great statistical difference between the cover and stego images, which indicates the proposed feature works well in detecting EA-LSBMR steganography.

III. EXPERIMENTAL RESULTS

A. Experimental setup

We randomly select 1000 images from the image databases NRCS [20] and UCID [21], respectively. In total, there are 2000 uncompressed color images. These images in databases NRCS are first center-cropped into small blocks with size of 512×512 and then all 2000 images are converted into gray-scale images.

In this paper, the AUC value which represents the area under the receiver operation characteristic (ROC) curve is used to evaluate the performance of steganalytic algorithms. The ROC curves of steganalyzers with only 1-D feature can be obtained by changing the classification threshold directly. While the ROC curves of all the steganalyzers with multi-dimensional features are got by support vector machine (SVM) classifier with the Gaussian kernel $k(x,y) = \exp\left(-\gamma \|x-y\|_2^2\right)$, $\gamma > 0$. The images are randomly divided into two equal parts, one for training and the other for testing. We use five-fold cross-validation on the training set to choose the best penalization parameter C and the kernel parameter γ in the following grid, and then use the trained classifier to classify the testing set.

$$\begin{cases} C \in \left\{2^i \middle| i = -5, \cdots, 15\right\} \\ \gamma \in \left\{2^j \middle| j = -15, \cdots, 3\right\}. \end{cases} \tag{4}$$

B. Comparison with the prior art

The algorithm in this paper is compared with the method proposed by Li et al. named LLPDF [14] and the subtractive pixel adjacency matrix (SPAM) method [15]. For our tests, all images are embedded at 10%, 20%, 30%, 40%, 50%, and 75% of the maximum embedding capacity using the EA-LSBMR steganography. We classify cover-images and stego-images using the algorithm proposed in this paper and the subtractive pixel adjacency matrix method.

TABLE I. AUC VALUES OF DIFFERENT STEGANALYZERS FOR EA-LSBMR WITH EMBEDDING RATES OF 10%, 20%, 30%, 40% AND 50%, RESPECTIVELY.

Data base	**algorith m**	**10%**	**20%**	**30%**	**40%**	**50%**
NRCS	LLPDF	0.5020	0.5122	0.5390	0.5709	0.6140
	SPAM	0.5032	0.5054	0.5078	0.5291	0.6036
	Proposed	**0.9909**	**0.9949**	**0.9911**	**0.9859**	**0.9938**
UCID	LLPDF	0.5161	0.5619	0.6481	0.7523	0.8434
	SPAM	0.5042	0.5115	0.5910	0.7230	0.8426
	Proposed	**0.9855**	**0.9784**	**0.9474**	**0.9109**	**0.9037**

Based on the minimal risk principle, the best classification threshold is obtained to classify the the features extracted using the proposed algorithm, while the features extracted by SPAM are classified using SVM classifier. Finally, we achieve the test results as shown in Tables 1.

From table I., we can see that the proposed steganalysis algorithm can effectively detect the existence of the hidden message especially in low embedding rate. Compared with LLTCF and SPAM, our proposed method performs the best under all circumstances.

IV. Conclusion

This paper proposes a targeted steganalysis method to defeat EA-LSBMR. For the EA-LSBMR steganography introduces abnormal fluctuations to the PVD histogram of the stego image, the PVD histogram of a stego-image will abnormally decrease on the threshold *T* and increase on the position of *T*+1. A steganalytic feature set is characterized through analyzing the differences of the PVD histograms between the cover and stego images. Experimental results show that the detecting performances of our proposed method are relatively better comparing with previous steganalysis algorithms. In future works, the proposed specific steganalysis will be researched to detect other adaptive steganography that designed based on the differences of consecutive pixel pairs.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (No. 60903221, 61272490). The authors would like to thank the reviewers for their insightful comments and helpful suggestions.

References

[1] A. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” in *Proc. 3rd Int. Workshop on Information Hiding*, vol. 1768, 1999, pp.61–76.

[2] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color, and gray-scale images,” *IEEE Multimedia*, vol. 8, pp. 22–28, Oct. 2001.

[3] S. Dumitrescu, X.Wu, and Z.Wang, “Detection of LSB steganography via sample pair analysis,” *IEEE Trans. Signal Process*, vol. 51, pp. 1995–2007, Jul. 2003.

[4] A. D. Ker, “A general framework for structural steganalysis of LSB replacement,” in *Proc. 7th Int. Workshop on Information Hiding,* Barcelona, 2005, vol. 3427, pp. 296–311.

[5] T. Sharp, “An implementation of key-based digital signal steganography,”in *Proc. 4th Information Hiding Workshop*, Berlin, 2001, pp. 13-26.

[6] J. J. Harmsen, W. A. Pearlman, “Steganalysis of additive noise modelable information hiding,” in *Proc. SPIE Security, Steganography, and Wartermarking of Multimedia Contents*, Bellingham, 2003, pp. 131-142.

[7] A. D. Ker, “Steganalysis of LSB matching in grayscale images,” *IEEE Signal Processing Letters*, vol. 12, pp. 441-444, Jun. 2005.

[8] J. Zhang, I. J. Cox and G. Doërr , “Steganalysis for LSB matching in images with high-frequency noise,” in *Proc. IEEE Workshop on Multimedia Signal Processing* . Piscataway, 2007, pp. 385-388.

[9] F. Huang, B. Li, and J. Huang, “Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels,” in *Proc.IEEE Int. Conf. Image Processing*, San Antonio, 2007, pp. 401-404.

[10] X. Li, T. Zeng, and B. Yang, “Detecting LSB matching by applying calibration technique for difference image,” in *Proc. 10th ACM Workshop on Multimedia and Security*, Oxford, 2008, pp. 133–138.

[11] T. Zhang, W. X. Li, and Y. Zhang, “Steganalysis of LSB matching based on statistical modeling of pixel difference distributions,” *Information Sciences*, vol. 180, pp. 4685-4694, Dec. 2010.

[12] K. Cai, X. Li, and T. Zeng, “Reliable histogram features for detecting LSB matching,” in *Proc. IEEE International Conference on Image Processing*, Piscataway, 2010, pp. 1761-1764.

[13] Y. Wang, P. Moulin, “Optimized feature extraction for learning-based image steganalysis,” *IEEE Trans. Information Forensics and Security*, vol. 2, pp. 31-45, Mar. 2007.

[14] B. Li, J. Huang, and Y Q. Shi, “Textural features based universal steganalysis,” in *Proc. SPIE Security, Forensics, Steganography and Watermarking of Multimedia*, Bellingham, 2008, pp. 1201-1212.

[15] T. Pevný, P. Bas, J. Fridrich, “Steganalysis by subtractive pixel adjacency matrix,” *IEEE Trans. on Information Forensics and Security*, vol. 5, pp. 215-224, Jun. 2010.

[16] G. Xiong, X.J. Ping, and T. Zhang, “Image textural features for steganalysis of spatial domain steganography,” *J. Electron. Imaging*, vol. 21: 033015-1-033015-15, Aug. 2012.

[17] J. Mielikainen, “LSB matching revisited,” *IEEE Signal Process. Lett.*, vol. 13, pp. 285-287, May. 2006.

[18] W. Q. Luo, F. J. Huang and J. W. Huang, “Edge Adaptive Image Steganography Based on LSB Matching Revisited,” *IEEE Trans.Information forensics and security*, vol.5 , pp.201-214, Jun. 2010.

[19] S.Q. Tan, “Steganalysis of LSB matching revisited for consecutive pixels using B-spline functions,” in *Proc. of the 10th International Workshop on Digital Forensics and Watermarking*, New Jersey, 2012, pp.16-29.

[20] [DB/OL]. http://photogallery.nrcs.usda.gov/.

[21] G. Schaefer , M. Stich UCID , “An Uncompressed Colour Image Database,” in Proc. of SPIE Storage and Retrieval Methods and Applications for Multimedia, Bellingham, 2004, pp. 472-480.