Computers, Materials & Continua CMC, vol.62, no.2, pp.963-976, 2020

An Adaptive Image Calibration Algorithm for Steganalysis

Xuyu Xiang[1], Jiaohua Qin[1, *], Junshan Tan[1] and Neal N. Xiong[1]

Abstract: In this paper, a new adaptive calibration algorithm for image steganalysis is proposed. Steganography disturbs the dependence between neighboring pixels and decreases the neighborhood node degree. Firstly, we analyzed the effect of steganography on the neighborhood node degree of cover images. Then, the calibratable pixels are marked by the analysis of neighborhood node degree. Finally, the strong correlation calibration image is constructed by revising the calibratable pixels. Experimental results reveal that compared with secondary steganography the image calibration method significantly increased the detection accuracy for LSB matching steganography on low embedding ratio. The proposed method also has a better performance against spatial steganography.

Keywords: Calibration algorithm, neighborhood node degree, ordinary pixel, sensitive pixel, steganalysis.

1 Introduction

Steganography is to achieve the purpose of covert communication by embedding information into innocuous-looking cover objects [Qin, Xiang, Deng et al. (2014)]. There are some kinds of literature such as describing sensitive statistical methods for reliable detection of LSB replacement [Dumitrescu, Wu and Wang (2003); Park, Han, Moon et al. (2016); Ker (2007); Niu, Sun, Qin et al. (2009)]. Dumitrescu et al. [Dumitrescu, Wu and Wang (2003)] detect the LSB steganography by the analysis of sample pair. Park et al. [Park, Han, Moon et al. (2016)] use the bit-plane decomposition to detect the LSB replacement. Ker [Ker (2007)] and Niu et al. [Niu, Sun, Qin et al. (2009)] put forward the steganalysis of LSB replacement to detect two least significant bits.

Also, some researchers focus on detecting the LSB matching steganography [Ker (2005); Liu, Sung and Ribeiro (2008); Abolghasemi, Aghainia and Faez (2008); Yu and Babaguchi (2008); Zhang, Hu and Yuan (2009); Xia, Sun and Qin (2009); Lerch-Hostalot and Megias (2013); Chen, Gao, Liu et al. (2016); Qin, Xiang and Wang (2010)]. Ker [Ker (2005)] construct the calibration image by using a downsampled image to improve the detection of LSB matching steganography. Liu et al. [Liu, Sung and Ribeiro (2008)] detect the LSB matching by analysis the image complexity. Abolghasemi et al. [Abolghasemi, Aghainia and Faez (2008)] detect the LSB matching by the co-occurrence matrix. Yu et al. [Yu and Babaguchi (2008)] use Run length to detect the LSB Matching.

[1] College of Computer Science and Information Technology, Central South University of Forestry & Technology, Changsha, 410114, China.

[2] Department of Mathematics and Computer Science, Northeastern State University, OK, 74464, USA.

[*] Corresponding Author: Jiaohua Qin. Email: qinjiaohua@163.com.

Zhang et al. [Zhang, Hu and Yuan (2009)] use the Envelope of Histogram to detect the LSB Matching. Xia et al. [Xia, Sun and Qin (2009)] use the Neighbourhood Node Degree Histogram to detect the LSB Matching. Lerch-Hostalot et al. [Lerch-Hostalot and Megias (2013)] proposed the LSB matching steganalysis by patterns of pixel differences. Chen et al. [Chen, Gao, Liu et al. (2016)] use characteristic function moment of pixel differences to detect the LSB Matching. Qin et al. [Qin, Xiang and Wang (2010)] present a review of detection of LSB matching steganography.

The difficulty of steganalysis is that there is no original image for comparative detection. If we can find a good method to construct a reference image similar to the original cover image, it will be very helpful for steganalysis.

Fridrich [Fridrich (2004)] constructs "calibrated" image by using the cropping and recompression image. She believes that the cropped stego image is perceptually similar to the cover image and its DCT coefficients have approximately the same statistical properties as the cover image. Ker [Ker (2005)] construct the calibration image by using a downsampled image to improve the detection of LSB matching steganography. Holotyak et al. [Holotyak, Fridrich and Soukal (2005)] uses the wavelet denoising method to estimate the cover image from the stego image, and estimate the secret message length for ±k embedding steganography. These are the more common processing methods at present. However, wavelet denoising and the downsampled image methods do not specifically consider the special application of steganography, and the algorithm complexity is large, and the actual effect is general, and the method of re-steganography is adopted [Yu and Babaguchi (2008); Xia, Sun and Qin (2009); Cancelli, Doerr, Cox et al. (2008)]. Although the Xia's method [Xia, Sun and Qin (2009)] achieves better detection performance than the Ker's [Ker (2005)] and Yu's [Yu and Babaguchi (2008)] methods, the applicability of the detection algorithm is very limited. Therefore, a targeted steganography image calibration technique is needed.

Recently, researchers have put forward some new improved LSB matching steganography [Soleimanpour-Moghadam and Nezamabadi-Pour (2016); Hiary, Sabri, Mohammed et al. (2016); Sahu and Swain (2018); Tan, Qin, Xiang et al. (2019); Liu, Wang, Zhang et al. (2014); Qin, Li, Xiang et al. (2019)]. Tan et al. [Tan, Qin, Xiang et al. (2019)] proposed the channel coding can use to the steganophy. Soleimanpour et al. [Soleimanpour-Moghadam and Nezamabadi-Pour (2016)] proposed pair-wise LSB matching steganography and Hiary et al. [Hiary, Sabri, Mohammed et al. (2016)] proposed a hybrid steganography system. Sahu et al. [Sahu and Swain (2018)] proposed an improved LSB Matching by combining bit differencing. Xia et al. [Xia and Li (2017)] even proposed the coverless LSB information hiding. Xiang et al. [Xiang, Li, Hao et al. (2018)] use synonym substitution and arithmetic coding to achieve the natural language steganography. Li et al. [Li, Qin, Xiang et al. (2018)] proposed the image matching algorithm can use to the steganography.

Liu et al. [Liu, Wang, Zhang et al. (2014)] proposed the feature selection method and Qin et al. [Qin, Li, Xiang et al. (2019)] proposed the improved Harris algorithm to extract features and used the BOW (Bag of Words) model to generate the feature vectors also can use to the steganophy.

Therefore, steganalysis is a long-term and arduous task. In this paper, we propose an

adaptive calibration method for image steganalysis. To begin with, we analyzed the effect of steganography on the neighborhood degree of the cover image. Next, the calibratable pixels are marked by the analysis of the transformation between the ordinary pixel and sensitive pixel. At last, the strong correlation calibration image is obtained by revising the calibratable pixels. The obtained calibration image is used to extract relevant features for steganalysis.

2 The proposed calibration approach

2.1 Calibration mechanism

Neighborhood degree: Let $p(i,j)$ be the pixel value of the image at the location (i,j). The neighborhood degree of the pixel (i,j) is defined as follows:

$$d(i,j)=\left\|\{(i+m,j+n)\mid p(i+m,j+n)=p(i,j)\}\right\| \tag{1}$$

where $\|\Delta\|$ denotes the cardinality of the set Δ, $\{\ \}$ is the set，$-\mathrm{K}\le m\le \mathrm{K},-\mathrm{K}\le n\le \mathrm{K}$, m and n cannot be zero at the same time. That is to say, only the K×K neighborhood is considered. The neighborhood degree $d(i,j)$ indicates the number of neighboring pixels which pixel value equals the $p(i,j)$.

Definition 1: Sensitive pixel set

Let S be the set of sensitive pixels of the image. We define the pixel (i,j) as the sensitive pixel if its neighborhood degree $d(i,j)\ge\delta$, $\{\ \delta$ is a threshold$\}$ then the sensitive pixel set S is defined as:

$$S=\left\{(i,j)\middle|\, d(i,j)\ge\delta\right\} \tag{2}$$

Definition 2: Ordinary pixel set

Let Θ be the set of ordinary pixels of the image. We define the pixel (i,j) as the ordinary pixel if its neighborhood degree $d(i,j)<\delta$, then the ordinary pixel set Θ is defined as:

$$\Theta=\left\{(i,j)\middle|\, d(i,j)<\delta\right\} \tag{3}$$

Definition 3: Calibratable pixel set

Let $\mathbb{R}$ be the set of calibratable pixels of the image. We define the pixel (i,j) as the calibratable pixel if the following conditions are satisfied:

$$\mathbb{R}_1=\left\{(i,j)\middle|(i,j)\in S\wedge\exists p(i,j)',\ p(i,j)-K\le p(i,j)'\le p(i,j)+K\ s.t\ d(i,j)'>d(i,j)\right\} \tag{4}$$

$$\mathbb{R}_2=\left\{(i,j)\middle|(i,j)\in \Theta\wedge\exists p(i,j)',\ p(i,j)-K\le p(i,j)'\le p(i,j)+K\ s.t\ (i,j)'\in S\right\} \tag{5}$$

Then the calibratable pixel set $\mathbb{R}$ is defined as:

$$\mathbb{R}=\left\{(i,j)|(i,j)\in\mathbb{R}_1\vee(i,j)\in\mathbb{R}_2\right\} \tag{6}$$

By definition, we can see that, if the pixel $(i,j)\in\Theta$, then the correlation between the pixel (i,j) and the surrounding pixels is weak; if the pixel $(i,j)\in \mathrm{S}$, then the correlation between the pixel (i,j) and adjacent pixels is very strong. The minor steganography changes of sensitive pixels will be reflected on the neighborhood degree. The sensitive

pixels most likely become ordinary pixels after steganography. Therefore in the process of calibration, we may consider the transformation between the ordinary pixel and sensitive pixel. Neighborhood degree value for calibration ordinary pixels within a subtle change is regarded as due to intensity changes induced by the natural image.

For the embedding operation of spatial steganography, the general steganography algorithm is to modify the last bit planes of the image, so the search range of calibration can be reduced appropriately $\pm K$, instead of searching all possible pixel values. This can reduce the amount of search and reduce the time complexity of the algorithm. After determining the search range, the calibratable pixel set $\mathbb{R}$ can be determined by the calibratable pixels. Then, the calibration image can be constructed by the adaptive image calibration algorithm.

The adaptive image calibration algorithm is as follows:

Algorithm: Adaptive Image Calibration

Input: image $I = \left(p(i,j) \right)_{h \times w}$

Output: the calibration image $I' = \left(p(i,j)' \right)_{h \times w}$

Steps:

1: for i = 1, . . . , h do
2: for j=1, … , w do
3: Calculate the neighborhood degree $d(i,j)$ by Eq. 1
4: Judge $(i,j) \in S$ or $(i,j) \in \Theta$ by Eq.(2) and Eq. 3
5: Search the neighborhood pixels of (i,j) by pixel value $p(i,j) \pm K$
6: if $(i,j) \in \mathbb{R}$ by Eq.(6) then
7: Record the pixel (i,j) and the $p(i,j)'$ which make (i,j) be calibratable pixel
8: $p(i,j) = p(i,j)'$
9: end if
10: end for
11: end for

The algorithm judge whether the pixel is a calibratable pixel or not, find all pixels which may be modified and modify it to be the pixel which makes the neighborhood increases. The calibration algorithm does not use the complex frequency domain transform. Therefore, its computational speed is very fast, the algorithm's time complexity is $O(t^2)$, and the space complexity is also $O(n^2)$. The calibration algorithm is more practical than the other.

2.2 Analysis of the calibration

To observe the calibration results, we test the Lena image of 100% LSB matching steganography embedding, the peak signal-to-noise rate (PSNR) of LSB matching

steganography image is 43.62, and the PSNR of the calibrated image is 43.97, so the PSNR of calibration stego image by our calibration algorithm is close to the original image.

The original image is modified by steganography, the neighborhood degree of the image is reduced, so many calibratable points may be generated during the calibration process, and the normal original image calibratable points are relatively few. We know steganography disturbs the dependence between neighboring pixels and decreases the neighborhood degree. So after calibration, a strong dependence "cover image" can be obtained.

Effects of the calibration ratio for cover image and stego image

The actual test is carried out by two image libraries NRCS and FreeFOTO, in which NRCS contains 3,162 uncompressed images, and FreeFOTO library contains 10,408 compressed images. In the experiments, we found that the calibration ratio changed greatly for original and stego image. The average statistics value of the calibration ratio for original and stego image has been calculated the proportion of the total pixels. It is shown in Fig. 1.

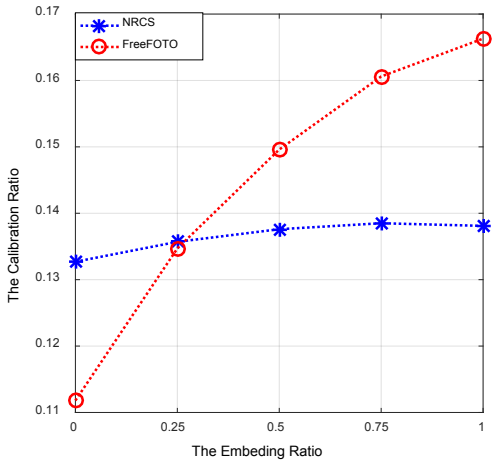


Figure 1: The statistics of the calibration ratio for original and stego image

From Fig. 1, we know that the ratio of the calibratable pixels for stego image is larger than the cover image, especially for compression images. It is a good feature for steganalysis.

Effects of the sum of the calibration histogram difference

As is known to all, the histogram is an effective and commonly used statistical feature for steganalysis. Because steganography has a smooth effect on the histogram of the image, in the process of steganographic image calibration, we record the pixel values modified by the calibration algorithm and calculate the difference between these pixel values and the surrounding pixel values. We find that the difference in the cover image is greater than the difference of the stego image. This also is a good steganalysis feature

The sum of calibration histogram difference is shown in Fig. 2.

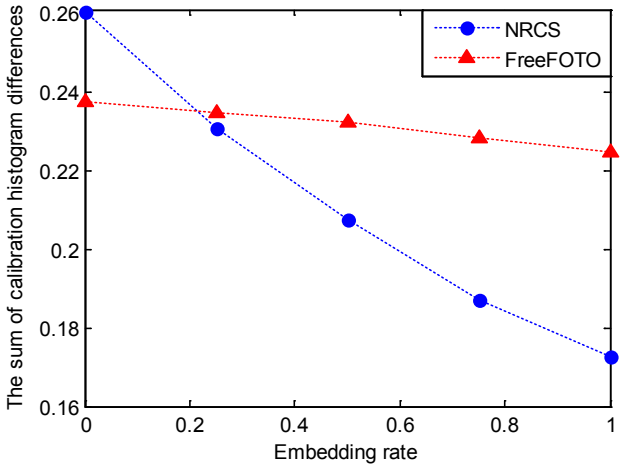


Figure 2: The sum of calibration histogram difference

2.3 Feature extraction

From the centroid of the neighborhood degree histogram, three features are extracted: $C(h(x))$, $C(h^{'}(x))$, R. Then two features $SumD$ and CR are computed by Eq. (9) and Eq. (10) respectively. Six features with the differential and DCH. For $C(h(x))$, $C(h^{'}(x))$, R, we calculate them once using 3×3 and 5×5 neighborhood respectively once by, so that a total of 9 features are used for steganalysis.

Center of Mass (COM) of NDH: First we define the neighborhood degree histogram (NDH): $h(x)=|\{(i,j)\,|\,d(i,j)=x\}|$, $h_c(x)$ and $h_s(x)$ denote the NDH of cover image and stego image respectively. The COM of NDH is defined as follows:

$$C(h(x))=\frac{\sum_{x=0}^{n} xh(x)}{\sum_{x=0}^{n} h(x)} \tag{7}$$

where n is the maximum of the NDH, $n=\begin{cases}8 & if\ k=1\\ 24 & if\ k=2\end{cases}$. After the LSB matching embedding, the neighborhood degree is reduced. Therefore, there are $C(h_c(x))>C(h_s(x))$. let $C^{'}(h(x))$ be the COM of NDH after embedding and denote the alteration rate of NDH COM as

$$R=\frac{C^{'}(h(x))-C(h(x))}{C(h(x))} \tag{8}$$

Due to LSB matching steganography, the stego image's alteration rate is greater than the cover image's thus $R_s>R_c$. Now the three features $C(h(x))$, $C^{'}(h(x))$ and R are calculated

through Eq. (7) and Eq. (8). Additionally, compute these features twice using 3×3 and 5×5 neighborhood respectively for a given image.

The sum of the neighborhood degree of image pixels is defined,

$$SumD = \sum d(i, j) \tag{9}$$

According to the calibration algorithm, the $SumD$ of an image reduces after LSB matching, i.e., $SumD_c > SumD_s$.

To value the calibration process, the calibration change ratio (CR) is defined as follows,

$$CR = \frac{Calibratable\ Pixels}{Total\ Pixels} \tag{10}$$

According to the calibration algorithm, the CR of an image increase after LSB matching, i.e., $CR_c < CR_s$.

Because of the LSB matching smoother the histogram, the sum of difference of the calibration histogram (DCH) is calculated as follows:

$$DCH = \frac{\sum_{i \in R_p} |H(i) - H(i+1)| + |H(i) - H(i-1)|}{\sum_{j=0}^{255} H(j)} \tag{11}$$

where R_p is the pixel value changed in the calibration, $H(n)$ is the calibration image's histogram thus define as $H(n) = \left|\{p(i, j) \mid p(i, j) = n\}\right|$. After LSB matching, the DCH is likely to decrease, namely $DCH_c > DCH_s$.

According to our observation, CR and DCH are two effective features that can be added to the feature vector. Finally, the feature vector composed of eight features are constructed for classification.

3 Classifier

Because of the good classification performance of support vector machine, we choose it with the non-linear kernel (RBF) as the classifier in our experiments.

Before training with classifiers, we normalize the features. For the feature, we calculate its maximum value and minimum value for training images. For any training image and test image, the feature F_i is extracted and scaled as

$$\widetilde{F_i} = \frac{F_i - F_{i\min}}{F_{i\max} - F_{i\min}},\ i = 1, 2, \cdots, 8 \tag{12}$$

where $F_{i\max}$ represents the maximum value and $F_{i\min}$ is the minimum value in F_i, respectively.

4 Experiments

4.1 Image data sets

The accuracy of steganalysis varies greatly from different image sources, so in our experiment, we use two image data sets to test the performance of the proposed algorithm and compare the performance with other methods.

In the experiment, we use two image sets with uncompressed and compressed images respectively.

NRCS Set: 3,162 high-resolution TIFF images are downloaded from http://photogallery.nrcs.usda.gov; all the images are uncompressed with size 2100×1500 or 1500×2100. For testing, we resample the images to 640×418 and convert it to grayscale.

FreeFOTO Set: 10,408 JPEG images are downloaded from http://www.freefoto.com. All the images are compressed with quality factor 75 and with size 600×400 or 400×600. For testing, we also convert this image into grayscale before use.

All of the above images were utilized as covers to generate stego images with LSB replacement, 2LSB replacement, LSB matching, BPCS steganography [Spaulding, Noda and Shirazi (2002)] and so on. The message lengths take 100%, 75%, 50% and 25% of the maximal embedding length (i.e., one bit per pixel). Therefore, for every Steganography, NRCS Set consists of 3,162×(1+4)=15,810 cover and stego images, and FreeFOTO Set consists of 10,408×(1+4)=52,040 images.

4.2 Training and testing image sets

Each image set above was divided into two parts: training and testing sets, to train and test the classifiers. The training image sets and testing image sets are composed of the 40% cover images and corresponding stego images randomly selected from the image data sets.

For NRCS Set, the training set contains 1,264 cover images and corresponding 5,056 stego images. Among the stego images, images of four embedding rates 100%, 75%, 50%, and 25%, are included. The test image set includes 1,898 cover images and 7,592 stego images with four embedding rates. Similarly, for FreeFOTO Set, the training image set is composed of 4,163 cover images and corresponding 16,652 stego images. The test image set is made up of 4,163×(1+4)=20,815 images.

4.3 Detection performance

The Receiver Operation Characteristic (ROC) curve is selected to show the detection probability based on the false positive probability.

To evaluate the detection effect of the ROC curve, the AUC (Area Under the ROC Curve) [Qin, Xiang and Wang (2010)] is defined as follows:

$$AUC = \int_0^1 P_D\left(P_{FP}\right) dP_{FP} \tag{13}$$

where P_D is the probability of detection, P_{FP} is the probability of false positive.

Detection performances are evaluated by 'detection reliability' ρ defined as [Fridrich (2004)]

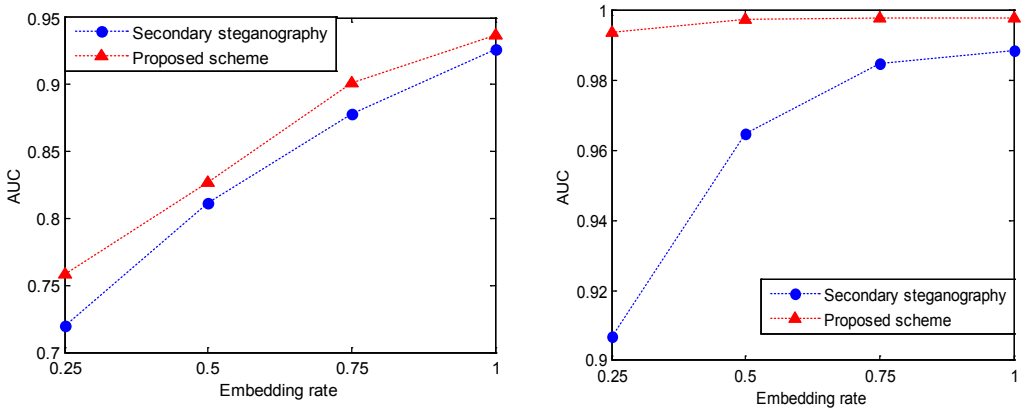
$$\rho = 2A - 1 \tag{14}$$

where A is the area under the receiver operating characteristic (AUC) curve. In this paper, the ROC curve is represented by plotting true detection probability versus false alarm probability.

4.4 Detection results

In this section, two groups of experiments are compared. The first group is to compare the proposed adaptive calibration method with the second steganography calibration method. The other group is to compare the proposed method with other spatial steganography algorithms. LSB matching is used to generate images with different embedding rates in different image libraries, which is used to test the effect of LSB matching steganalysis with the proposed adaptive calibration and secondary steganographic calibration methods.

The AUC for the uncompressed images in NRCS and compressed images in FreeFOTO are shown in Fig. 3(a) and Fig. 3(b), where the four different abscissa points from left to right represent the message embedding rates of 100%, 75%, 50% and 25% with LSB matching, respectively.

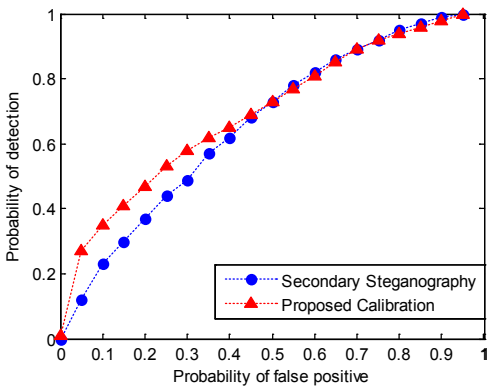


(a) AUC for NRCS (b) AUC for FreeFOTO

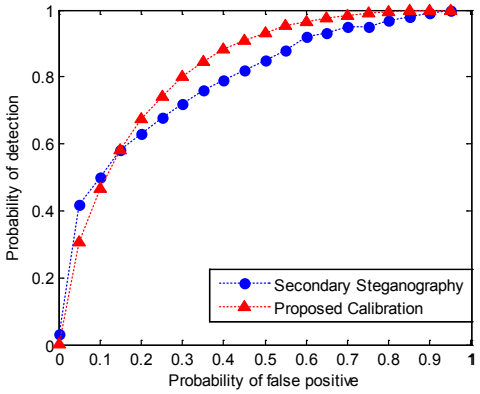
Figure 3: AUC Comparison with Secondary steganography and the proposed calibration for NRCS and FreeFOTO sets

Fig. 3 shows that the detection results are more accurate with the proposed calibration method in both compressed and uncompressed image sets. Therefore, the image calibration algorithm based on neighborhood degree can be used in LSB matching steganography detection and the detection accuracy is improved.

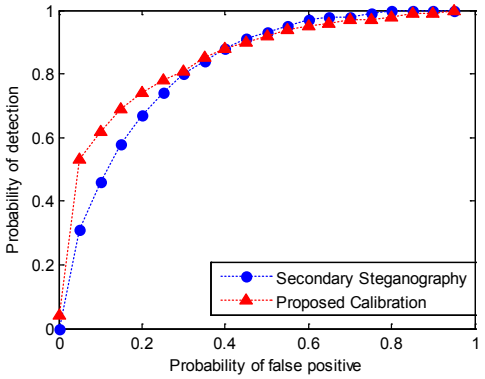
Some ROC curves of detection performances are shown in Fig. 4 and Fig. 5, The detection reliabilities ρ of all methods are compared in Fig. 6.



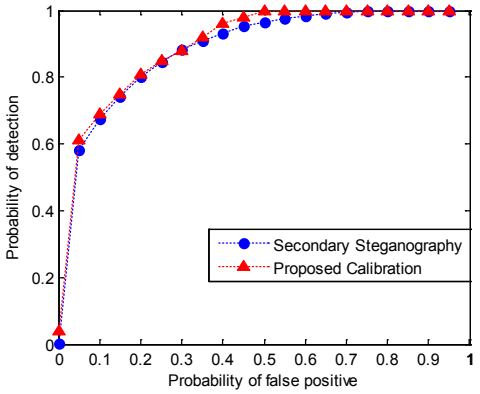
(a) NRCS 25%



(b) NRCS 50%

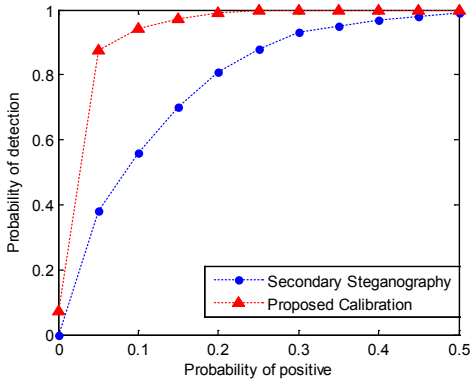


(c) NRCS 75%

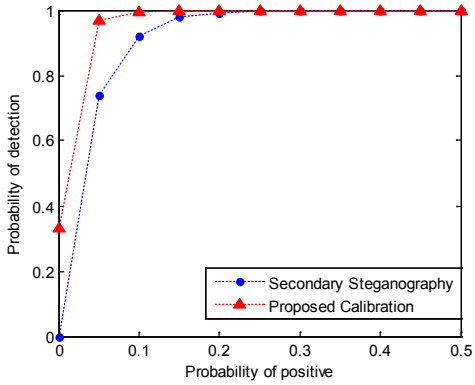


(d) NRCS 100%

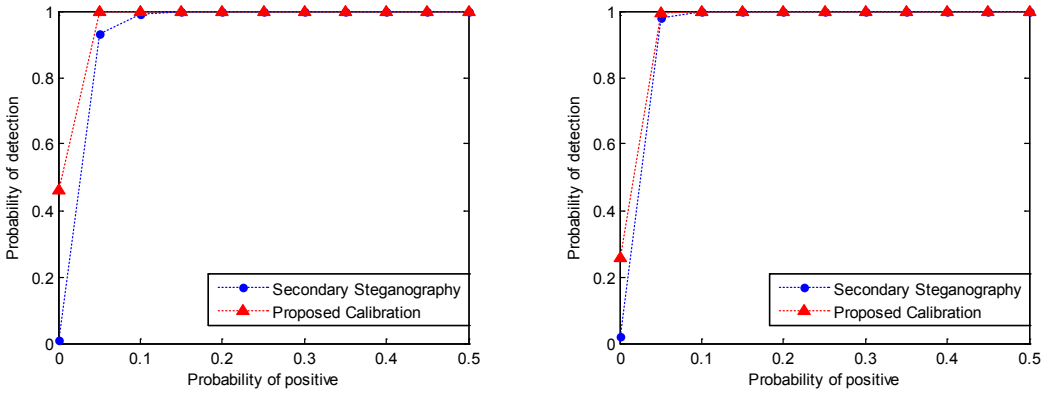
Figure 4: ROC of NRCS set for four embedding rates Comparison with Secondary steganography and the proposed calibration scheme



(a) FreeFOTO 25%



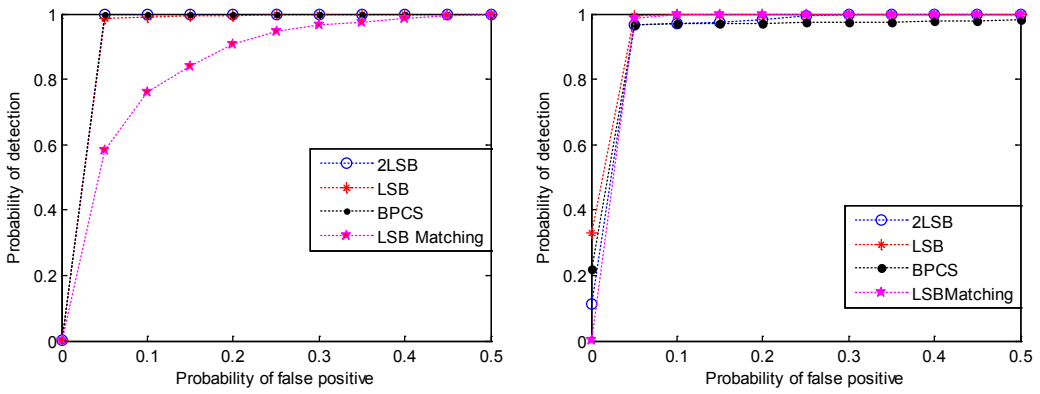
(b) FreeFOTO 50%



(c) FreeFOTO 75% (d) FreeFOTO 100%

Figure 5: ROC of FreeFOTO set for four embedding rates Comparison with Secondary steganography and the proposed calibration

Compared with the proposed adaptive calibration with the secondary steganography from Fig. 4 and Fig. 6, the experimental results show that the adaptive calibration algorithm significantly increased the detection results for LSB matching steganography with low embedding ratio in both compressed and uncompressed image sets.



(a) NRCS (b) FreeFOTO

Figure 6: Detection reliabilities of four different methods with adaptive calibration

As can be seen from Fig. 6, the adaptive calibration algorithm can effectively detect the steganography in the spatial domain. Whether the steganography based on bit plane or visual characteristics, the detection efficiency for LSB matching is the worst in the uncompressed image database, which also shows that the LSB matching is better than other steganography from the side. Although the 2LSB steganography avoids the histogram pairing phenomenon of LSB substitution, the adaptive calibration loss caused

by much modification pixel is higher than LSB substitution, so the detection result of 2LSB steganography is the best.

5 Conclusions

In this paper, a new image construction method using adaptive calibration against spatial steganography is proposed. Firstly, we analyze the effects of LSB matching on the neighborhood degree for the cover image. Secondly, the calibratable pixels are found by the analysis of neighborhood degree, and the calibration image is reconstructed. Finally, features are extracted and used to train the support vector machine. The proposed adaptive calibration method is efficient to detect the LSB matching steganography on low embedding ratio and also to detect the other spatial steganography. It is a research hotspot to image steganalysis with deep learning. At the same time, some coverless steganography appears, and this is a challenge to the steganalyzers. Our future work is to research the coverless steganography and steganalysis with deep learning.

Acknowledgment: This work is supported by the National Natural Science Foundation of China (No. 61772561), the Key Research & Development Plan of Hunan Province (No. 2018NK2012), the Key Laboratory for Digital Dongting Lake Basin of Hunan Province.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Abolghasemi, M.; Aghainia, H.; Faez, K. (2008): Steganalysis of LSB matching based on co-occurrence matrix and removing most significant bit planes. *4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1527-1530.

Cancelli, G.; Doerr, G.; Cox, I. J.; Barni, M. (2008): Detection of ±1 LSB steganography based on the amplitude of histogram local extrema. *International Conference Image Processing*, pp. 1288-1291.

Chen, X. Y.; Gao, G. Y.; Liu, D. D.; Xia, Z. H. (2016): Steganalysis of LSB matching using characteristic function moment of pixel differences. *China Communications*, vol. 13, no. 7, pp. 66-73.

Dumitrescu, S.; Wu, X. L.; Wang, Z. (2003): Detection of LSB steganography via sample pair analysis. *IEEE Transactions on Signal Processing*, vol. 51, no. 7, pp. 1995-2007.

Fridrich, J. (2004): Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. *6th Information Hiding Workshop*, pp. 67-81.

Hiary, H.; Sabri, K. E.; Mohammed, M. S.; Al-Dhamari, A. (2016): A hybrid steganography system based on LSB matching and replacement. *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 9, pp. 374-380.

Holotyak, T. S.; Fridrich, J.; Soukal, D. (2005): Stochastic approach to secret message length estimation in ±k embedding steganography. *SPIE Electronic Imaging*, pp. 673-684.

Ker, A. D. (2005): Steganalysis of LSB matching in grayscale images. *IEEE Signal Process Letters*, vol. 12, no. 6, pp. 441-444.

Ker, A. D. (2007): Steganalysis of embedding in two least significant bits. *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 46-54.

Lerch-Hostalot, D.; Megias, D. (2013): LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers and Security*, vol. 32, pp. 192-206.

Li, H.; Qin, J. H.; Xiang, X. Y.; Pan, L. L.; Ma, W. T. et al. (2018): An efficient image matching algorithm based on adaptive threshold and RANSAC. *IEEE Access*, vol. 6, no. 1, pp. 66963-66971.

Liu, Q.; Sung, A. H.; Ribeiro, B. (2008): Image complexity and feature mining for steganalysis of least significant bit matching steganography. *Information Sciences*, vol. 178, no. 1, pp. 21-36.

Liu, X. W.; Wang, L.; Zhang, J.; Yin, J. P.; Liu, H. (2014): Global and local structure preservation for feature selection. *IEEE Transactions on Neural Networks and Learning Systems*, vol. 25, no. 6, pp. 1083-1095.

Niu, C. M.; Sun, X. M.; Qin, J. H.; Xia, Z. H. (2009): Steganalysis of two least significant bits embedding based on least square method. *International Conference on Computing, Communication, Control and Management*, pp. 124-127.

Park, T. H.; Han, J. G.; Moon, Y. H.; Eom, I. K. (2016): Performance improvement of LSB-based steganalysis using bit-plane decomposition of images. *Imaging Science Journal*, vol. 64, pp. 262-266.

Qin, J. H.; Li, H.; Xiang, X. Y.; Tan, Y.; Pan, W. Y. et al. (2019): An encrypted image retrieval method based on Harris corner optimization and LSH in cloud computing. *IEEE Access*, vol. 7, no. 1, pp. 24626-24633.

Qin, J. H.; Xiang, X. Y.; Deng, Y.; Li, Y. Y.; Pan, L. L. (2014): Steganalysis of high undetectable steganography using convolution filtering. *Information Technology Journal*, vol. 13, no. 16, pp. 2588-2592.

Qin, J. H.; Xiang, X. Y.; Wang, M. X. (2010): A review on detection of LSB matching steganography. *Information Technology Journal*, vol. 9, no. 8, pp. 1725-1738.

Sahu, A. K.; Swain, G. (2018): An improved data hiding technique using bit differencing and LSB matching. *Internetworking Indonesia*, vol. 10, no. 1, pp. 17-21.

Soleimanpour-Moghadam, M.; Nezamabadi-Pour, H. (2016): The pair-wise LSB matching steganography with a discrete quantum behaved gravitational search algorithm. *Journal of Intelligent and Fuzzy Systems*, vol. 30, no. 3, pp. 1547-1556.

Spaulding, J.; Noda, H.; Shirazi, M. N. (2002): BPCS steganography using EZW lossy compressing images. *Pattern Recognition Letters*, vol. 23, no. 13, pp. 1579-1587.

Tan, Y.; Qin, J. H.; Xiang, X. Y.; Ma, W. T.; Pan, W. Y. et al. (2019): A robust watermarking scheme in YCbCr color space based on channel coding. *IEEE Access*, vol. 7, no. 1, pp. 25026-25036.

Xia, B.; Sun, X. M.; Qin, J. H. (2009): Steganalysis based on neighbourhood bode degree histogram for LSB matching steganography. *International Conference on Multimedia Information Networking and Security*, pp. 79-82.

Xia, Z. H.; Li, X. (2017): Coverless information hiding method based on LSB of the character's unicode. *Journal of Internet Technology*, vol. 18, no. 6, pp. 1353-1360.

Xiang, L. Y.; Li, Y.; Hao, W.; Yang, P.; Shen, X. B. (2018): Reversible natural language watermarking using synonym substitution and arithmetic coding. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 541-559.

Yu, X. Y.; Babaguchi, N. (2008): Run length based steganalysis for LSB matching steganography. *IEEE International Conference on Multimedia and Expo*, pp. 353-356.

Zhang, J.; Hu, Y. P.; Yuan, Z. B. (2009): Detection of LSB matching steganography using the envelope of histogram. *Journal of Computers*, vol. 4, no. 7, pp. 646-653.