

A Learning-Based Steganalytic Method against LSB Matching Steganography

Zhihua XIA¹, Lincong YANG², Xingming SUN^{*1}, Wei LIANG¹, Decai SUN¹, Zhiqiang RUAN¹

¹Hunan Provincial Key Laboratory of Network and Information Security, Hunan University, Changsha, 410082, China

²School of Journalism and Communication, Hunan University, Changsha, 410082, China

xia_zhihua@163.com, lincongyanghu@163.com, sunnudt@163.com, idlink@163.com, sdecai@163.com,
rzq_911@163.com

*Corresponding author: Xingming SUN, Tel.: 86-731-88821341; fax: 86-731-88822417

Abstract. *This paper considers the detection of spatial domain least significant bit (LSB) matching steganography in gray images. Natural images hold some inherent properties, such as histogram, dependence between neighboring pixels, and dependence among pixels that are not adjacent to each other. These properties are likely to be disturbed by LSB matching. Firstly, histogram will become smoother after LSB matching. Secondly, the two kinds of dependence will be weakened by the message embedding. Accordingly, three features, which are respectively based on image histogram, neighborhood degree histogram and run-length histogram, are extracted at first. Then, support vector machine is utilized to learn and discriminate the difference of features between cover and stego images. Experimental results prove that the proposed method possesses reliable detection ability and outperforms the two previous state-of-the-art methods. Further more, the conclusions are drawn by analyzing the individual performance of three features and their fused feature.*

Keywords

Communication security, steganalysis, histogram gradient energy, neighborhood degree histogram, run-length histogram, support vector machine.

1. Introduction

As the development of public communication network, plenty of information can be easily transmitted all over the world, which has brought much attention to the communication security. Many early methods exploited encryption techniques to prevent unauthorized access. However, the encrypted form may arouse special suspicion of network warders [1]. Steganographic techniques are developed to deceive warders by embedding messages into cover objects in an imperceptible manner. The purpose of steganography is to transmit secret messages through public communication channel without being suspected.

In the process of embedding, the cover object is slightly modified to conceal the secret data. The modified object, named as stego object, could be sent to the receiver through the public communication network. The receiver then uses the corresponding extraction method to get the secret data from the stego object. Steganalysis, the opponent to steganography, is used to prevent the baleful secret communication by detecting the existence of the hidden message in a given object. Generally speaking, if an algorithm can judge whether a given object contains a secret message or not, the steganographic system is considered broken by this algorithm [2]. In this paper, we concentrate on the detection of spatial domain LSB matching steganography in gray images.

During the process of LSB matching, if the LSB of the image pixel matches the secret data bit, it will leave the pixel unchanged. Otherwise, the pixel will be added or subtracted by one at random. LSB matching has the advantages including high payload, good visual imperceptibility and extremely easy implementation as LSB replacement. What's more, it is harder to be detected than its counterpart since it avoids the histogram asymmetry in LSB replacement [3-4].

The existing detection methods against LSB matching steganography can be classified into two categories. One is named as special detector that designs an elaborated feature and configures a threshold value to distinguish stego images from the original ones. The other one is the learning-based detector (also referred as universal detector) which extracts multiple sensitive features from sample database to train a classifier that is used to detect the presence of hidden message [5].

For special detector, Harmsen and Pearlman modeled the effect of message embedding as the disturbance of additive pulse noise and utilized center of mass of histogram characteristic function (*HCF COM*) to detect the hidden message [6]. This method had been proved efficient in the detection of LSB replacement for RGB color bitmaps, however, ineffective for LSB matching in grayscale images [7]. Ker improved Harmsen's method by two ways: 1) computing the 2D adjacency histogram instead of usual

histogram, 2) using a down-sampled image as a calibration version of the test image [7]. Compared with the original *HCF COM*, significant improvements were achieved. Fridrich et al. [8] proposed a maximum likelihood estimator to estimate the message length. However, it is found that the approach is powerless for never-compressed images derived from a scanner. To solve the problem of detecting images with large noise component, Zhang et al. [9] exploited the change of local extremum of image histogram caused by message embedding, which obtained an improved result. However, the performance is comparatively poor when the method is utilized to detect the images that are compressed by JPEG-compressor.

With regard to learning-based detectors, Goljan et al. [10] extracted features from the wavelet domain to train classifiers. Liu et al. [11] exploited the correlation of least and second significant bit plane to attack LSB matching and revealed that the accuracy of the classifier degenerates as the image complexity increases. Pevny et al. [12] argued that the dependence between neighboring pixels were disturbed by message embedding, and utilized Markov model to extract sensitive features. Xu et al. [13] and Cancelli et al. [14] utilized the histogram distortions caused by LSB matching to extract multiple histogram features. Based on the fact that LSB matching only influences the two LSB bit planes of image, Mehrabi et al. removed the most significant bits of the image so as to improve the detection performance [15].

The key of both special and learning-based detector is to design discriminating features. Existing features are always based on a certain inherent property of images which are likely to be disturbed by message embedding. For instance, ref. [5], [6], [8], [13], [14] concentrated on the distortion of image histogram caused by LSB matching, while ref. [7], [9]-[12], [15] designed the features mainly based on dependence among the image pixels. Image histogram and pixel dependence are the two distinct image properties, and thus are expected to have their own strong-point in detection of hidden message. Therefore, the distortion of the two properties should be observed to reveal hidden message.

In this paper, a learning-based steganalysis method against LSB match steganography is proposed. In the light of statements above, three features are extracted to train support vector machine (SVM) classifiers. Firstly, LSB matching is modeled as adding an additive pulse noise to the image. As a result, image histogram will become smoother. Histogram gradient energy is calculated so as to reveal this change. Secondly, the neighboring pixels of image usually exhibit high dependence with each other. Based on this, images are divided into overlapped sub-images and neighborhood degree histogram is devised to consider this type of dependence. Thirdly, regarding the dependence among pixels that are not adjacent to each other, run-length histogram is constructed to deal with it. As well as the joint investigation, these features are tested separately to reveal their individual advantages in the de-

tection of uncompressed and JPEG-compressed images.

The rest of the paper is organized as follows. Section 2 describes the feature extraction process. In section 3, the support vector machine is introduced briefly. Experiments are presented in section 4. Conclusions are drawn in section 5.

2. Feature Extraction

In this work, steganalysis is considered as a binary classification problem, i.e. classifying the testing image either a stego or an original image. The framework of training and testing process of binary classification is illustrated in Fig. 1. From each image, features are extracted to form a feature vector which is used as the representation of corresponding image. Feature vector sets are obtained by extracting features from image sets, and then used to train classifier.

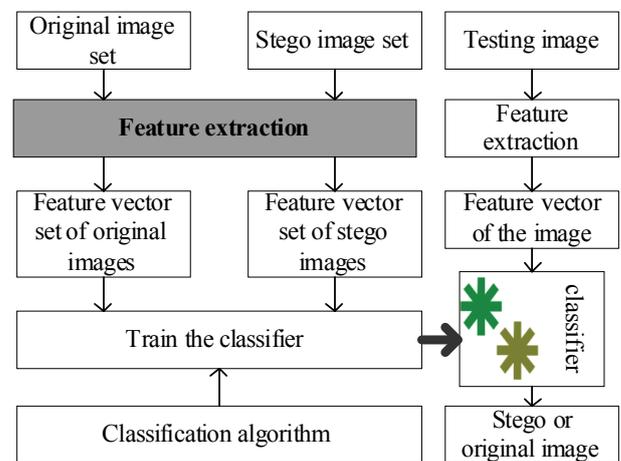


Fig. 1. The framework of training and testing process of binary classification.

Feature extraction is a key step for pattern classification. As mentioned earlier, natural images have some inherent properties, such as histogram, dependence between neighboring pixels, and dependence among pixels that have distance larger than one. Based on these properties, three features are extracted in this section, including histogram gradient energy (*HGE*), center of mass of neighborhood degree histogram (*NDH COM*) and center of mass of run-length histogram (*RLH COM*).

2.1 Embedding Strategy of LSB Matching

Define the grayscale image as a 2D array I , where $0 \leq I(i, j) \leq 2^L - 1$, $0 \leq i \leq M - 1$, $0 \leq j \leq N - 1$. Here, $L = 8$ for the gray images; M and N represent the image dimension. Denote a stego image as I_s and its corresponding cover images as I_c . Note that the subscripts 's' and 'c' are used to indicate the symbol version corresponding to stego and cover image respectively in this paper. Assume b is a secret message bit. The embedding strategy of LSB matching is formulated as follows.

$$I_s(i, j) = \begin{cases} I_c(i, j), & I_c(i, j) \bmod 2 = b \\ I_c(i, j) \pm 1, & I_c(i, j) \bmod 2 \neq b \text{ \& } 0 < I_c(i, j) < 255 \\ I_c(i, j) + 1, & I_c(i, j) \bmod 2 \neq b \text{ \& } I_c(i, j) = 0 \\ I_c(i, j) - 1, & I_c(i, j) \bmod 2 \neq b \text{ \& } I_c(i, j) = 255 \end{cases} \quad (1)$$

Note that the pixel will be added or subtracted at random by one in the case of $I_c(i, j) \bmod 2 \neq b \text{ \& } 0 < I_c(i, j) < 255$.

2.2 HGE

Define the histogram of a gray image as $h(n) = |\{I(i, j) \mid I(i, j) = n\}|$, and $p, 0 \leq p \leq 1$ as the embedding rate. According to embedding strategy of LSB matching, a pixel will be changed with probability of $p/2$ after LSB matching, increasing or decreasing by one both with the probability of $p/4$. The effects of LSB matching on image histogram can thus be formulated as follows.

$$\begin{cases} h_s(n) = (1 - \frac{p}{2})h_c(n) + \frac{p}{4}h_c(n-1) + \frac{p}{4}h_c(n+1), \\ \quad \quad \quad n \in \{2 \dots 253\}, \\ h_s(0) = (1 - \frac{p}{2})h_c(0) + \frac{p}{4}h_c(1), \\ h_s(1) = (1 - \frac{p}{2})h_c(1) + \frac{p}{2}h_c(0) + \frac{p}{4}h_c(2), \\ h_s(254) = (1 - \frac{p}{2})h_c(254) + \frac{p}{4}h_c(253) + \frac{p}{2}h_c(255), \\ h_s(255) = (1 - \frac{p}{2})h_c(255) + \frac{p}{4}h_c(254) \end{cases} \quad (2)$$

Under this situation, LSB matching will be deduced as low pass filter on the histogram with the kernel of $[p/4, 1-p/2, p/4]$ if histogram boundary is ignored. Namely, histogram will be smoothed by the LSB matching. In this paper, HGE is calculated to characterize this effect as follows.

$$HGE = \sum_{i=0}^{254} |h(i) - h(i+1)|. \quad (3)$$

Using HGE_c and HGE_s to denote the HGE of the cover and stego images, respectively, we have

$$HGE_s \leq HGE_c. \quad (4)$$

Proof:

Under the assumption that the boundary elements of histogram are quite small, we write the formula (2) as its approximation.

$$\begin{cases} h_s(n) = (1 - \frac{p}{2})h_c(n) + \frac{p}{4}h_c(n-1) + \frac{p}{4}h_c(n+1), \\ \quad \quad \quad n \in \{1 \dots 254\}, \\ h_s(0) = (1 - \frac{p}{2})h_c(0) + \frac{p}{2}h_c(1), \\ h_s(255) = (1 - \frac{p}{2})h_c(255) + \frac{p}{2}h_c(254) \end{cases} \quad (2')$$

Write

$$\begin{aligned} HGE_s &= \sum_{i=0}^{254} |h_s(i) - h_s(i+1)| \\ &= |h_s(0) - h_s(1)| + \sum_{i=1}^{253} |h_s(i) - h_s(i+1)| \\ &\quad + |h_s(254) - h_s(255)| \end{aligned} \quad (5)$$

Firstly, based on formula (2'), we derive

$$\begin{aligned} &\sum_{i=1}^{253} |h_s(i) - h_s(i+1)| \\ &= \sum_{i=1}^{253} \left| \left(1 - \frac{p}{2}\right)[h_c(i) - h_c(i+1)] + \right. \\ &\quad \left. \frac{p}{4}[h_c(i-1) - h_c(i)] + \frac{p}{4}[h_c(i+1) - h_c(i+2)] \right| \\ &\leq \left(1 - \frac{p}{2}\right) \sum_{i=1}^{253} |h_c(i) - h_c(i+1)| \\ &\quad + \frac{p}{4} \sum_{i=1}^{253} |h_c(i-1) - h_c(i)| + \frac{p}{4} \sum_{i=1}^{253} |h_c(i+1) - h_c(i+2)| \\ &= \left(1 - \frac{p}{2}\right) \sum_{i=1}^{253} |h_c(i) - h_c(i+1)| \\ &\quad + \frac{p}{4} \sum_{i=0}^{252} |h_c(i) - h_c(i+1)| + \frac{p}{4} \sum_{i=2}^{254} |h_c(i) - h_c(i+1)| \end{aligned} \quad (5-1)$$

Secondly, according to the formula (2') we have the following as well

$$\begin{aligned} |h_s(0) - h_s(1)| &\leq \left(1 - \frac{p}{2}\right) |h_c(0) - h_c(1)| \\ &\quad + \frac{p}{4} |h_c(0) - h_c(1)| + \frac{p}{4} |h_c(1) - h_c(2)| \end{aligned} \quad (5-2)$$

$$\begin{aligned} |h_s(254) - h_s(255)| &\leq \left(1 - \frac{p}{2}\right) |h_c(254) - h_c(255)| \\ &\quad + \frac{p}{4} |h_c(254) - h_c(255)| + \frac{p}{4} |h_c(253) - h_c(254)| \end{aligned} \quad (5-3)$$

Finally, according to the formulas (5-1), (5-2) and (5-3), we obtain $HGE_s \leq HGE_c$. **Proof End.**

2.3 NDH COM

Dependence between adjacent pixels has been taken into consideration in the 3×3 overlapped sub-images, each of which can be regarded as a neighborhood $N(i, j)$ with a center pixel $I(i, j)$ as it is illustrated in Fig. 2.

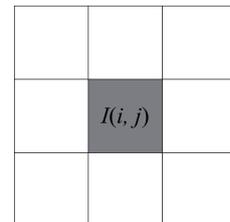


Fig. 2. 3×3 neighborhood $N(i, j)$ with center pixel $I(i, j)$.

The neighborhood degree is defined as the number of pixels that have equal gray value with the center pixel in the said neighborhood, and is formulated as:

$$ND(i, j) = |\{I(i+u, j+v) | I(i+u, j+v) = I(i, j)\}| \quad (6)$$

where $(u, v) \in \{(-1, -1), (-1, 0), (-1, 1), (0, -1), (0, 1), (1, -1), (1, 0), (1, 1)\}$.

The neighborhood degree can be considered as an indicator to the pixel dependence in the corresponding neighborhood. To be more specifically, the larger the degree is, the greater dependence that is held by the neighborhood will be. After LSB matching, neighborhood holding a relatively large degree is likely to decrease in number. To describe this phenomenon, we define the neighborhood degree histogram (NDH) as follows

$$NDH(x) = |\{N(i, j) | ND(i, j) = x\}|, x = 0, 1, \dots, 8. \quad (7)$$

Fig. 3 shows the change of NDH of the ‘lena’ image after LSB matching with maximal message length. Intuitively, elements of NDH move towards the side with smaller degree after message embedding. Consequently, the center of mass of the NDH (NDH COM) is calculated as a discriminating feature.

$$COM(NDH(x)) = \frac{\sum_{x=0}^8 xNDH(x)}{\sum_{x=0}^8 NDH(x)}. \quad (8)$$

According to the analysis above, the NDH COM of an image decreases after LSB matching, i.e.

$$COM(NDH_s(x)) < COM(NDH_c(x)). \quad (9)$$

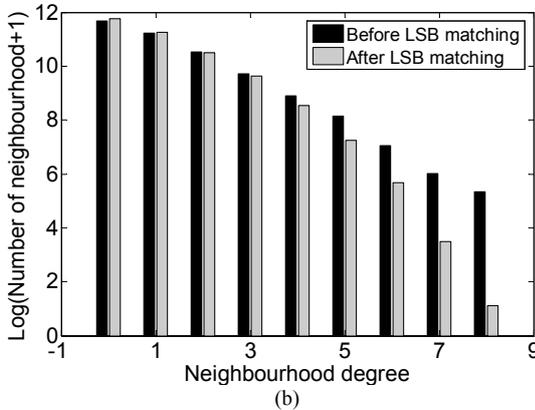
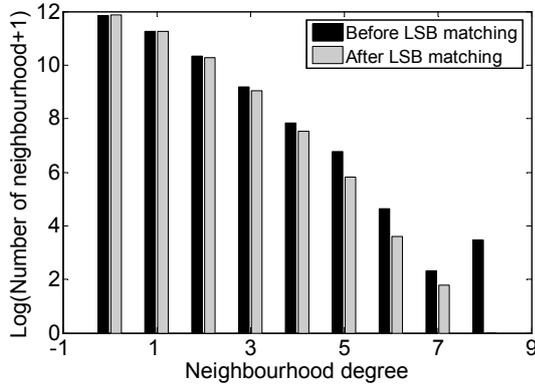


Fig. 3. NDH of the ‘lena’ image before and after LSB matching with maximal message length: (a) uncompressed ‘lena’ image, (b) JPEG-compressed ‘lena’ image with quantization quality of 75.

2.4 RLH COM

This paper utilizes the run-length histogram (RLH) [16] to extract the feature which catches dependence among pixels that have the distance larger than one. Scanning the image in a mode, a run is a set of consecutive image pixels with equal intensity, and the run length is defined as the amount of pixels in the run [17]. Then, run-length histogram is a 1D array whose elements, $RLH(x)$, is equal to the number of run with the length of x in an image.

After LSB matching, the run with long length is likely to be divided in to several shorter ones, and thus the RLH changes as it is illustrated in Fig. 4. Define the center of mass of RLH (RLH COM) as:

$$COM(RLH(x)) = \frac{\sum_{x=0}^n xRLH(x)}{\sum_{x=0}^n RLH(x)} \quad (10)$$

where n is the length of the longest run. After LSB matching, the RLH COM of image is also likely to be decreased, namely,

$$COM(RLH_s(x)) < COM(RLH_c(x)). \quad (11)$$

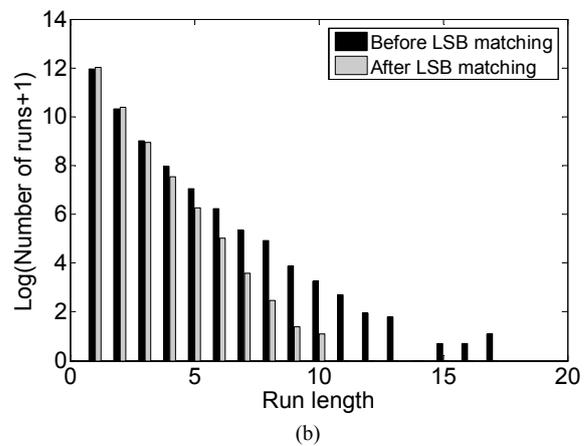
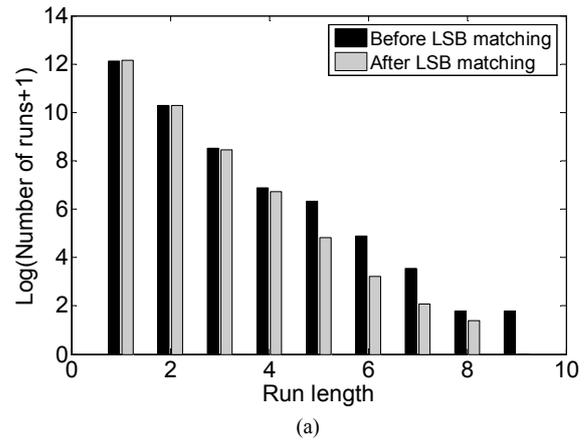


Fig. 4. RLH of the ‘lena’ image before and after LSB matching with maximal message length: (a) uncompressed ‘lena’ image, (b) JPEG-compressed ‘lena’ image with quantization quality of 75.

2.5 Calibration Mechanism and Normalization

Natural images are highly various, and so do the features extracted from these images. Thus, the feature distortion caused by message embedding is likely to be obscured

by the variability of features. To solve this problem, we choose to use calibration mechanism which aims at minimizing the noise caused by message embedding and to keeping the general properties of the image unchanged at the same time [18]. In this paper, we utilize the wavelet transform to calibrate features as it is illustrated in Fig. 5.

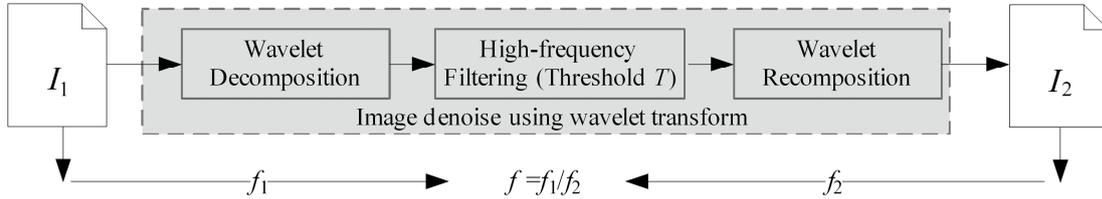


Fig. 5. The flow chart of feature calibration with wavelet transform.

After the calibration, the features need to be normalized in order to obtain comparable dynamic ranges. For a calibrated feature f , its maximum value f_{\max} and minimum value f_{\min} is found from the whole images set at first. Then, feature f is normalized by

$$f' = \frac{f - f_{\min}}{f_{\max} - f_{\min}}. \quad (12)$$

The normalization prevents the features with large numerical range from dominating those features with small numerical ranges, and thus avoids numerical ill-conditioning [19].

3. Support Vector Machine

SVM is utilized to train the classifier in this paper. Considering input data as two sets of vectors in an n -dimensional space, SVM constructs an optimal separating hyperplane by Lagrangian multipliers so as to distinguish the positive data points from the negative ones [20]. Intuitively, a good separation is achieved by the hyperplane that has the greatest distance to the neighboring points of both classes.

LIBSVM [21] is an integrated software for support vector classification, regression, and distribution estimation. With regard to support vector classification, LIBSVM implements four basic kernels among which RBF kernel is suggested as the best choice by the developers. LIBSVM also provides some useful tools, among which the tool “Cross-validation and Grid-search” can be used to search the appropriate penalty parameter C and kernel parameter γ for RBF kernel. In addition, LIBSVM provides a tool to draw ROC (receiver operating characteristics) curve and calculate the AUC (area under the ROC curve) for binary classification application. LIBSVM is directly used to train classifiers with the extracted features in this paper.

4. Experiments

Extensive experiments are conducted on two image

sets in this section. Firstly, the detection performances of the three features, i.e. *HGE*, *NDH COM* and *RLH COM*, are tested separately. Secondly, these features are summed up as a fused feature whose performance is also discussed. Thirdly, these features are combined to construct a “joint feature set” to train SVM classifiers to attack the LSB matching steganography. In addition, we implement Ker’s [7] and Liu’s [11] methods to facilitate performance comparisons. Note that we configured experimentally the threshold of wavelet denoising $T=4$ in the process of feature calibration, and we scanned the images both horizontally and vertically when calculating *RLH COM*.

4.1 Image Sets

The accuracy of steganalysis varies significantly across different image sources. In particular, images with large noise component are more challenging for steganalysis than images with low noise component (such as JPEG-compressed images) [12]. In order to evaluate the proposed method, the experiments are conducted separately on two sets with uncompressed and JPEG-compressed images contained respectively.

Set#1: 3,162 uncompressed images downloaded from NRCS [22]. The images are digital TIFF files with the size either 2100×1500 or 1500×2100 . The images are cut to 525×375 or 375×525 and are converted to grayscale ones before being used.

Set#2: 10,408 images downloaded from FreeFOTO [23]. These 600×400 or 400×600 sized images were converted to grayscale images which were then compressed and decompressed by JPEG-compressor with the quantization quality of 75.

All above images were utilized as covers to generate stego images with LSB matching steganography. The message lengths take 100%, 75%, 50% and 25% of the maximal embedding length (i.e. one bit per pixel). Therefore, Set#1 consists of $3,162 \times (1+4) = 15,810$ cover and stego images, and Set#2 consists of $10,408 \times (1+4) = 52,040$ images.

4.2 Configuration of SVM Classifiers

Training and testing image sets: Each image set above was divided into two parts: training and testing sets, to train and test the classifiers. For Set#1, the training set contains 2,000 cover images and 2,000 corresponding stego images. Among the 2,000 stego images, images of four embedding rates, i.e. 100%, 75%, 50% and 25%, are equally included. The test image set includes 1,162 cover images and stego images with four message lengths (i.e. $1,162 \times 4 = 4,648$ stego images). Similarly, for Set#2, the training image set is composed of 6,000 cover images and 6,000 corresponding stego images. The test image set is made up of $4,408 \times (1+4) = 22,040$ images.

Parameters of SVM: *C*-support vector classification (*C*-SVC) of the LIBSVM with RBF kernel was utilized to train classifiers in the experiments, and the tool named as ‘‘Cross-validation and Grid-search’’ was used to search the penalty parameter *C* and kernel parameter γ . For the two image set, the parameter pairs (*C*, γ) used in Liu’s and our methods (joint feature set) are listed in Tab. 1.

Methods	Image set	
	Set#1	Set#2
Liu’s method	(2, 16384)	(1,8)
Joint feature set	(2, 4)	(1024,1)

Tab. 1. Parameter pairs (*C*, γ) of SVM.

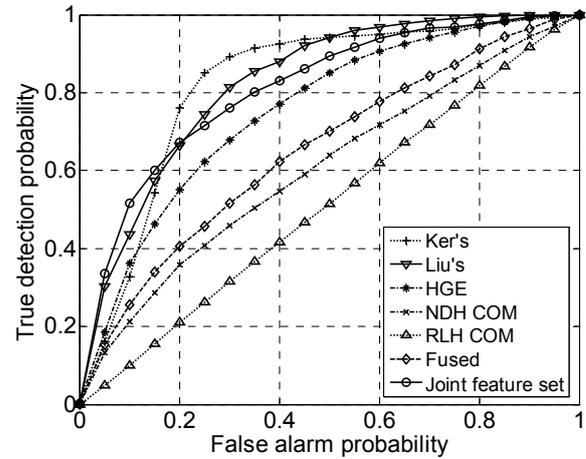
4.3 Detection Results

Detection performances are evaluated by ‘detection reliability’ ρ [18] defined as

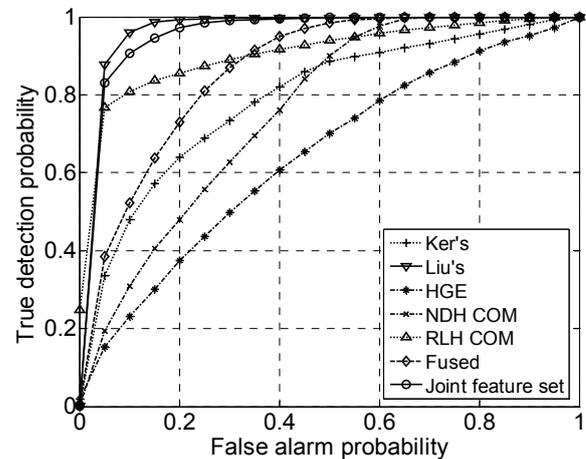
$$\rho = 2A - 1 \tag{13}$$

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

performances are presented in Fig. 6; while the detection reliabilities ρ of all methods are listed in Tab. 2.



(a) The detection of image set#1.



(b) The detection of image set #2.

Fig. 6. ROC curve samples, the embedding rate is 50%.

Image set	Embedding rates	Detection reliability						
		Ker’s	Liu’s	HGE	NDH COM	RLH COM	Fused feature	Joint feature set
Set#1	100%	0.8366	0.8420	0.8330	0.3326	0.0238	0.4418	0.9278
	75%	0.7884	0.8071	0.7208	0.2892	0.0290	0.3960	0.8366
	50%	0.6464	0.6549	0.5102	0.2138	0.0266	0.3022	0.6248
	25%	0.4168	0.3710	0.2616	0.1208	0.0098	0.1676	0.3278
	average	0.6720	0.6687	0.5814	0.2390	0.0224	0.3270	0.6792
Set#2	100%	0.9376	0.9931	0.5642	0.9244	0.8510	0.9376	0.9732
	75%	0.9052	0.9885	0.4622	0.7650	0.8468	0.9138	0.9637
	50%	0.5846	0.9608	0.2898	0.5212	0.8298	0.7324	0.9441
	25%	0.1346	0.8022	0.0630	0.2628	0.7316	0.3732	0.8855
	average	0.6406	0.9362	0.3448	0.6184	0.8148	0.7392	0.9416

Tab. 2. Detection reliabilities of methods.

4.4 Result Discussion

As it is shown in Tab. 2, *NDH COM* and *RLH COM* take advantage of the dependence among image pixels and are proved to be suitable to detect images with low noise, as images in set#2. *HGE* exploits the histogram change caused by message embedding and performs better on the uncompressed images. The joint feature set contains the three features which catch the message embedding effects both on image histogram and correlation, and thus holds the best detection results when compared with the detectors that utilize the single feature and the other two previous methods.

HGE is expected to obtain satisfying results for both compressed and uncompressed images since the histogram of both kinds of images will be smoothed by LSB matching. However, the detection accuracy of *HGE* for Set#2 can not compete with that for Set#1. The reason is that histogram becomes smoother after JPEG-compression (see Fig. 7). Therefore, the histogram distortion of JPEG-compressed images caused by LSB matching is weaker than that of uncompressed ones.

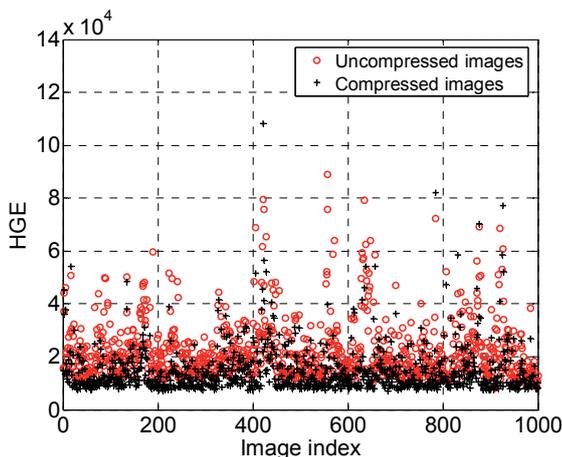


Fig.7. *HGE* of 1000 original images in Set#1 and their JPEG-compressed version (quantization quality is 75).

In addition, it can be observed that the fusion of features does not always ensure the improved performance. For example, the performance of the fused feature is inferior to that of *HGE* in the detection for Set#1, and can not compete with *RLH COM* for Set#2. Learning-based method is more suitable to deal with multiple features.

5. Conclusions

A learning-based steganalytic method has been presented to detect LSB matching steganography in gray images. Three features are extracted to form a joint feature set to train SVM classifiers for detection purpose. Experimental results demonstrate that the trained classifiers outperform the other two previous methods and the detectors utilizing the single feature. In addition, the individual performances of the three features are compared. According to

the experimental results, the *HGE* is suitable to detect uncompressed images, while *NDH COM* and *RLH COM* are good for the JPEG-compressed images.

The presented method is by no means optimal. Better models which can catch the distortion of image need to be devised in order to improve detection accuracy. For instance, increasing the dimensionality of feature set may be a feasible way.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 60736016, 60973128, 60973113, 61073191, 61070196, 61070195), National Basic Research Program 973 (Grant Nos. 2009CB326202, 2010CB334706), and Natural Science Foundation of Xiangtan (Grant No. 09JJ9006).

References

- [1] LIE, W.-N., LIN, G.-S. A feature-based classification technique for blind image steganalysis. *IEEE Transactions on Multimedia*, 2005, vol. 7, no. 6, p. 1007-1020.
- [2] FRIDRICH, J., GOLJAN, M. Practical steganalysis of digital images - State of the Art. In *Proc. Security and Watermarking of Multimedia Contents IV*. San Jose (USA, CA), 2002, p. 1-13.
- [3] KER, A. D. A general framework for structural steganalysis of LSB replacement. In *Proc. 7th International Workshop on Information Hiding*. Barcelona (Spain), 2005, p. 296-311.
- [4] LI, X. L., YANG, B., CHENG, D. F., ZENG, T. Y. A generalization of LSB matching. *IEEE Signal Processing Letters*, 2009, vol. 16, no. 2, p. 69-72.
- [5] LUO, X. Y., WANG, D. S., WANG, P., LIU, F. L. A review on blind detection for image steganography. *Signal Processing*, 2008, vol. 88, no. 9, p. 2138-2157.
- [6] HARMSEN, J. J., PEARLMAN, W. A. Steganalysis of additive noise modelable information hiding. In *Proc. Security and Watermarking of Multimedia Contents V*. Santa Clara (USA, CA), 2003, p. 131-142.
- [7] KER, A. D. Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, 2005, vol. 12, no. 6, p. 441-444.
- [8] FRIDRICH, J., SOUKAL, D., GOLJAN, M. Maximum likelihood estimation of length of secret message embedded using +/- K steganography in spatial domain. In *Proc. Security, Steganography, and Watermarking of Multimedia Contents VII*. San Jose (USA, CA), 2005, p. 595-606.
- [9] ZHANG, J., COX, I. J., DOERR, G. Steganalysis for LSB matching in images with high-frequency noise. In *Proc. IEEE Ninth Workshop on Multimedia Signal Processing*. Chania (Greece), 2007, p. 385-388.
- [10] GOLJAN, M., FRIDRICH, J., HOLOTYAK, T. New blind steganalysis and its implications. In *Proc. Security, Steganography, and Watermarking of Multimedia Contents VIII*. 2006, p. 7201-7201.
- [11] LIU, Q.Z., SUNG, A. H., RIBEIRO, B., WEI, M. Z., CHEN, Z. X., XU, J. Y. Image complexity and feature mining for steganalysis of least significant bit matching steganography. *Information Sciences*, 2008, vol. 178, no. 1, p. 21-36.
- [12] PEVNY, T., BAS, P., FRIDRICH, J. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 2010, vol. 5, no. 2, p. 215-224.

- [13] XU, M., LI, T., PING, X. Steganalysis of LSB matching based on histogram features in grayscale image. In *Proc. 11th IEEE International Conference on Communication Technology*. Piscataway (NJ, USA), 2008, p. 669-672.
- [14] CANCELLI, G., DOERR, G., COX, I. J., BARNI, M. Detection of \pm LSB steganography based on the amplitude of histogram local extrema. In *Proc. 15th IEEE International Conference on Image Processing*. Piscataway (NJ, USA), 2008, p. 1288-1291.
- [15] MEHRABI, M. A., AGHAEINIA, H., ABOLGHASEMI, M. Steganalysis of LSB-matching steganography by removing most significant bit planes. In *Proc. 2008 International Symposium on Telecommunications*. Tehran (Iran), 2008, p. 731-734.
- [16] YU, X. Y., BABAGUCHI, N. Run length based steganalysis for LSB matching steganography. In *Proc. IEEE International Conference on Multimedia and Expo*. Hannover (Germany), 2008, p. 353-356.
- [17] STABNO, M., WREMBEL, R. RLH: bitmap compression technique based on run-length and Huffman encoding. *Information Systems*, 2009, vol. 34, no. 4-5, p. 400-414.
- [18] FRIDRICH, J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In *Proc. 6th International Workshop Information Hiding*. Toronto (Canada), 2004, p. 67-81.
- [19] WANG, Y., MOULIN, P. Optimized feature extraction for learning-based image steganalysis. *IEEE Transactions on Information Forensics and Security*, 2007, vol. 2, no. 1, p. 31-45.
- [20] BURGESS, C. J. C. A tutorial on support vector machines for pattern recognition. *Data Mining and Knowledge Discovery*, 1998, vol. 2, no. 2, p. 121-167.
- [21] CHANG, C.-C., LIN, C.-J. *LIBSVM: a Library for Support Vector Machines*. [Online] Cited 2010. Available at: <http://www.csie.ntu.edu.tw/~cjlin/libsvm>.
- [22] NRCS. [Online] Cited 2008. Available at: <http://photogallery.nrcs.usda.gov>.
- [23] FreeFoto. [Online] Cited 2007. Available at: <http://www.freefoto.com>.

About Authors...

Zhihua XIA is currently pursuing his PhD in computer science and technology at the School of Computer and Communication of Hunan University, China. His research interests include Steganography and Steganalysis, digital forensic, image processing, and pattern recognition.

Lincong YANG received her master degree in 2001 from Central South University, China. She is now an associate professor in Hunan University.

Xingming SUN (Corresponding author) is currently a professor in Hunan University. His research interests include network and information security, digital watermarking, digital forensic, and natural language processing.

Wei LIANG is currently pursuing a Ph. D. candidate in Hunan University. His current research interests include real-time embedded systems, intellectual property protection, and field programmable gate arrays.

Decai SUN is currently pursuing his PHD in Hunan University, China. His main research interests are natural language processing, information retrieval, computational biology and pattern recognition.

Zhiqiang RUAN is currently pursuing a Ph. D. candidate in computer science from Hunan University. His current main research interests include security in wireless sensor networks and ad hoc system and network security.