Computers, Materials & Continua CMC, vol.62, no.3, pp.1259-1271, 2020

An Efficient Steganalysis Model Based on Multi-Scale LTP and Derivative Filters

Yuwei Chen[1, 2], Yuling Chen[1, *], Yu Yang[1, 2], Xinda Hao[2] and Ning Wang[2]

Abstract: Local binary pattern (LBP) is one of the most advanced image classification recognition operators and is commonly used in texture detection area. Research indicates that LBP also has a good application prospect in steganalysis. However, the existing LBP-based steganalysis algorithms are only capable to detect the least significant bit (LSB) and the least significant bit matching (LSBM) algorithms. To solve this problem, this paper proposes a steganalysis model called msdeLTP, which is based on multi-scale local ternary patterns (LTP) and derivative filters. The main characteristics of the msdeLTP are as follows: First, to reduce the interference of image content on features, the msdeLTP uses derivative filters to acquire residual images on which subsequent operations are based. Second, instead of LBP features, LTP features are extracted considering that the LTP feature can exhibit multiple variations in the relationship of adjacent pixels. Third, LTP features with multiple scales and modes are combined to show the relationship of neighbor pixels within different radius and along different directions. Analysis and simulation show that the msdeLTP uses only 2592-dimensional features and has similar detection accuracy as the spatial rich model (SRM) at the same time, showing the high steganalysis efficiency of the method.

Keywords: Image steganalysis, LTP, multi-scale, image residuals.

1 Introduction

Steganography is an information hiding technique that embeds secret information into a carrier without causing human perception. Nowadays, steganography is increasingly being used in privacy communications [Lei, Yang, Niu et al. (2017)]. However, in addition to being used for privacy protection, steganography can also be used to spread malicious messages. Therefore, in order to prevent the abuse of steganography, the steganalysis technology has also received more and more attention. After years of development, current mainstream steganalysis methods use the Spatial Rich Model (SRM) [Fridrich and Kodovský (2012)] and its derived algorithms or use machine learning-based techniques to detect whether images are steganized.

Recently, many studies have applied deep learning methods to steganalysis. These studies used convolutional neural networks to automatically extract image features for

[1] Guizhou University, Guizhou Provincial Key Laboratory of Public Big Data, Guiyang, 550025, China.

[2] Information Security Center, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[*] Corresponding Author: Yuling Chen. Email: ylchen3@gzu.edu.cn.

steganalysis. The deep learning-based approach aims to automatically extract features using machine learning methods instead of manual feature design. However, in the current research, the machine learning method cannot completely replace the manual features, especially the machine learning cannot simulate the quantification and interception process in the manual feature design. Therefore, it is still necessary to manually design the steganalysis features.

The spatial rich model (SRM) Fridrich et al. [Fridrich and Kodovský (2012); Holub and Fridrich (2013); Denemark, Sedighi, Holub et al. (2014); Tang, Li, Luo et al. (2016); Kodovský and Fridrich (2012); Goljan, Fridrich and Cogranne (2014)] is an advanced method for feature extraction of blind steganalysis. The method utilizes linear and non-linear filters to obtain various types of residuals to represent the relationship between adjacent pixels, thereby detecting whether the information has been embedded in the image. The SRM can detect steganography methods such as the least significant bit (LSB), the highly undetectable steganography (HUGO), and the edge adaptive algorithm (EA) with high accuracy. However, the SRM uses 34671-dimensional features. To deal with complex features makes the process of feature extraction and classification process very time-consuming and the detection process inefficient. Therefore, many studies [Yang, Chen, Chen et al. (2018)] tend to reduce the dimensions of the steganalysis features for better detection efficiency.

The local binary pattern (LBP) is an excellent image classification recognition operator that is commonly used in image texture detection. However, in recent years, some studies have pointed out that the LBP feature extraction method can also be applied to the field of image steganalysis. Ojala et al. [Ojala, Pietikäinen and Mäenpää (2000)] proposed a framework for steganalysis algorithms centered on the LBP feature extraction; Gui et al. [Gui, Li and Yang (2014)] applied it to the steganalysis algorithm for the LSBM; Lin et al. [Lin, Liu and Guo (2016)] extended it to the LTP (local ternary patterns) [Tan and Triggs (2010)] feature extraction algorithm to improve the accuracy of the steganalysis. Compared with the SRM, the LBP has a lower feature dimension and the detection performance has been greatly improved. However, most LBP-based steganalysis algorithms Tan et al. [Tan and Triggs (2010); Lafferty and Ahmed (2004)] can only detect the LSB and the MLSB algorithms, but cannot detect the steganography algorithms such as EA, HUGO and S-UNIWARD.

To solve these problems, this paper proposes a steganalysis model called msdeLTP.

The main contributions of this paper are as follows:

1. The residual analysis idea is introduced into the current LBP based methods. The current LBP based features are affected by the image content and cannot fully reflect the noise caused by the steganography. Therefore, the residuals of the image are first extracted to reduce the interference of the image content on the steganalysis, and the LBP based features are extracted from the residual images.

2. The multi-scale LTP is used as a feature for steganalysis. The single-scale feature can only reflect the changes of pixels adjacent to the central pixel, while the multi-scale mode enables the feature vector to better consider pixel variations in different neighborhoods, improving the detection effect of steganalysis. For this reason, a better scale combination is selected for the proposed multi-scale LTP steganalysis feature.

3. A modified Fisher efficiency is proposed in this paper to measure the performance of the feature. The common Fisher score is often used to measure the classification effect of features. For steganalysis, however, features are often used to reflect the impact of steganography on the image. The common Fisher score does not reflect this effect of the steganographic feature well, nor does it reflect the effect of the feature dimension on the classification efficiency. In order to better adapt to the steganalysis, we propose a modified Fisher efficiency based on the feature's modified Fisher score and feature dimension to measure the performance of the feature for steganalysis.

In the msdeLTP model, the ensemble classifiers are used to classify the features extracted from the images. Experiments show that the msdeLTP model has a small dimension feature and can ensure good detection accuracy.

The structure of this article is shown as follows. Section 2 introduces the proposed methods and the details of the selection of LBP mode and the derivative filters. Section 3 gives the simulation results of msdeLTP and analyzes the performance of the proposed method. Finally, in the fourth section we summarize the paper and give the future research direction.

2 The proposed algorithm

This paper proposes a steganalysis model based on the LBP and derivative filters. The model can detect a variety of non-adaptive steganography algorithms and adaptive steganography algorithms. First, in order to reduce the influence of image content on steganalysis, we studied and designed a set of derivative filters to extract the residual of the image. After that, we studied different basic patterns of LBP and selected the basic model with better classification ability while ensuring classification efficiency. Based on this, the multi-scale mode LTP is used to improve the detection capabilities of features. Finally, after extracting the multi-scale LTP features of the residual images, the ensemble classifiers are used to classify these features. The specific process of the msdeLTP model is shown in Fig. 1:

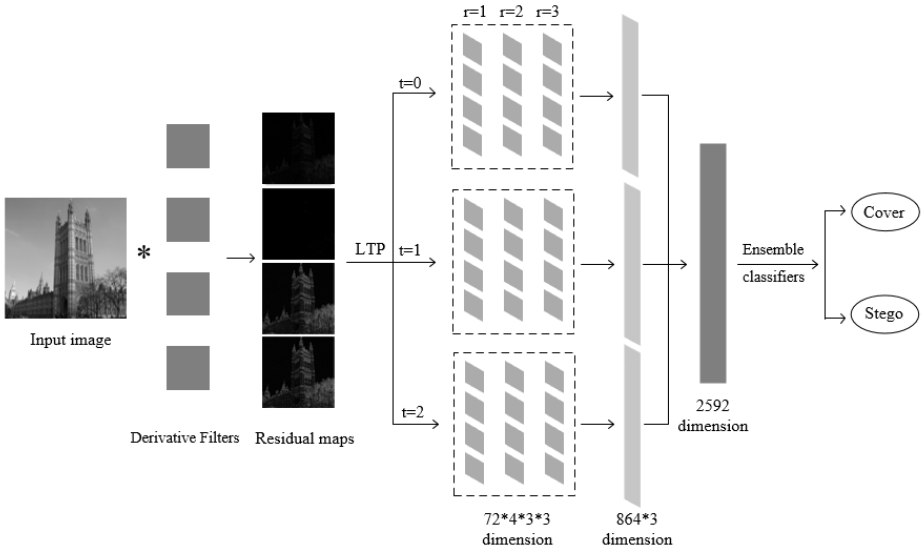

Figure 1: The process of the msdeLTP model

2.1 Design of the derivative filters

Modern advanced content adaptive steganography algorithms tend to change the texture regions of the image more, and make smaller changes to the smooth region of the image. In addition, the weak perturbation and image content noise caused by steganography is very small. Therefore, preprocessing that strengthens the stego signal is a very important step in the steganalysis process. The residual image is commonly used for this problem, because the residual image can reduce the influence of image content noise on the steganalysis, so that the extracted features are more related to the embedded information. In this paper, the derivative filters are used to obtain the residual images.

The derivative is a mathematical definition that captures the relationship between function values, and the derivative filter can also capture the relationship between adjacent pixels in different directions. The derivative filter can make the local region smooth, thereby magnifying the effects of embedding secret information.

For a two-dimensional image matrix $f(x,y)$, Eq. (1) can respectively represent the definition of the first derivative in the horizontal direction.

$$\frac{\partial f(\mathrm{x,y})}{\partial \mathrm{x}} = f(x,y) - f(x+1,y) \tag{1}$$

Thereby, it is possible to calculate derivative filters of different orders in the horizontal direction and the vertical direction. For example, in the nth order in the horizontal direction and the *m*-th order in the vertical direction, the derivative filter can be referred to as $\mathrm{D}_{n,m}$. The calculation formula of $\mathrm{D}_{n,m}$ is shown in the Eq. (2).

$$\frac{\partial^m}{\partial \mathrm{y}^m}\left(\frac{\partial^n f(x,y)}{\partial \mathrm{x}^n}\right) = \frac{\partial^{m-1}}{\partial \mathrm{y}^{m-1}}\left(\frac{\partial^n f(x,y)}{\partial \mathrm{x}^n}\right) - \frac{\partial^{m-1}}{\partial (\mathrm{y}+1)^{m-1}}\left(\frac{\partial^n f(x,y)}{\partial \mathrm{x}^n}\right) \tag{2}$$

It can be seen that the calculation of the derivative filter is similar to the calculation of the partial derivative.

In addition to this, it is also possible to obtain a filter having two directivities at the same time simply by convolving the derivative filters in different directions.

$$\mathrm{D}_{2,1} = \mathrm{D}_{2,0} \otimes \mathrm{D}_{0,1} = [-1 \quad 2 \quad -1] \otimes \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 & 2 & -1 \\ 1 & -2 & 1 \end{bmatrix} \tag{3}$$

In order to obtain residual images in different directions, the filter can be filled into a square to facilitate rotating the filter to different angles. The filled filter can be rotated at angles of 45°, 90°, 135°, 180°, 225°, 270°, and 315°.

In this paper, several different derivative filter combinations are selected to detect the influence of different derivative filter banks on the performance of steganalysis, and the influence of different number of derivative filters on the performance of steganalysis is also studied.

The filters banks we tested are shown in Tab. 1:

Table 1: Filters derived from different derivatives and their fill rotation

C1	C2	C3
$D_{1,0}^{0^\circ} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$D_{2,0}^{0^\circ} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix}$	$D_{2,1}^{0^\circ} = \begin{bmatrix} -1 & 2 & -1 \\ 1 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix}$
$D_{1,0}^{45^\circ} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$D_{2,0}^{45^\circ} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$D_{2,1}^{90^\circ} = \begin{bmatrix} 0 & 1 & -1 \\ 0 & -2 & 2 \\ 0 & 1 & -1 \end{bmatrix}$
$D_{3,0}^{0^\circ} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & -3 & 3 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$D_{4,0}^{0^\circ} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & -4 & 6 & -4 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$D_{4,2}^{0^\circ} = \begin{bmatrix} 1 & -4 & 6 & -4 & 1 \\ -2 & 8 & -12 & 8 & -2 \\ 1 & -4 & 6 & -4 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$
$D_{3,0}^{45^\circ} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$D_{4,0}^{45^\circ} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	$D_{4,2}^{90^\circ} = \begin{bmatrix} 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & -4 & 8 & -4 \\ 0 & 0 & 6 & -12 & 6 \\ 0 & 0 & -4 & 8 & -4 \\ 0 & 0 & 1 & -2 & 1 \end{bmatrix}$

In order to demonstrate the effect of the filters, we first compare the filtered image with the difference image of stego and cover image. In Fig. 2, the left image is the filtered stego image, and the right image is the difference image between stego and cover image. It can be seen that for adaptive steganography algorithms, the embedding position is usually at the edge of the image texture. Appropriate filters can extract image texture edges, allowing steganalysis to focus on these possible embedding positions while minimizing the impact of image content on steganalysis.

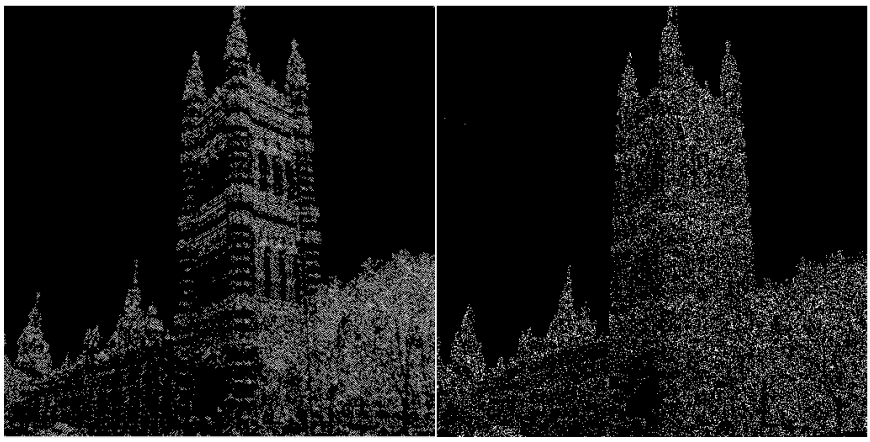

Figure 2: The comparison of the filtered stego image and the difference image between stego and cover image

In order to further improve the accuracy of the steganalysis, the impact of different filter banks on steganalysis were tested. As shown in Tab. 2, when the ri mode LBP is used and the steganography rate is fixed at 0.1, the detection error rate obtained by filtering the original image using the derivative filter is lower than when the LBP is used alone. From

this, it can be concluded that the use of a derivative filter is effective for improving the steganalysis ability of the LBP algorithm, and the performance of the LTP can be further improved in the case of using a plurality of combined filters. From the experiment results in Tab. 2, it can be expected that the more filters are combined in the experiment, the lower the error rate we will obtain. But at the same time, the dimension of the feature vector will become higher, and the downward trend of the error rate will gradually become smaller. Due to the limitations of time and experimental equipment, in order to simply verify the effect of the derivative filter, there is a tendency to use no more than four filter combinations.

Table 2: Error rate of derivative filter based steganalysis algorithm under different steganography algorithms and filter banks

ri, 0, 1	LTP	$D_{4,2}$	C1	C2	C3
LSBM	0.2008	0.1395	0.1056	0.1051	0.0867
EA	0.2303	0.2632	0.1531	0.1814	0.2274
HUGO	0.4396	0.3955	0.3697	0.3784	0.3303
S-UNIWARD	0.4414	0.3892	0.3964	0.3886	0.3306

2.2 Design of the LBP basic mode

The feature used in the msdeLTP model is the LTP feature of the multi-scale mixed resolution mode. This feature is based on the LBP. Therefore, in order to design better features, the LBP basic mode that is most suitable for steganalysis needs to be selected.

The LBP is a commonly used texture detection feature and can also be used in steganalysis. In the following, the definition of the LBP and the three basic modes of LBP are briefly introduced. In the traditional square LBP mode, when taking the 3×3 neighborhood as an example, the LBP algorithm compares the gray value of the center point and that of the eight adjacent points around it. If the gray value of the adjacent point is smaller than the gray value of the center pixel, the adjacent pixel is marked with 0, otherwise the pixel is marked with 1. The resulting 8-bit binary string is converted to a decimal value ranging from 0 to 255. Do all the bits in the image as the center pixel for the same operation (the edge must be treated specially). By counting all the decimal numbers obtained, a histogram with 256 bins can be obtained, and the distribution of the histogram can represent the texture information of the entire image. The mathematical formula for the LBP is defined as:

$$\text{LBP} = \sum_{P=0}^{P-1} s(g_p - g_c)2^p \tag{4}$$

where $g_p, p = 1,2,\ldots,$ 8 are 8 neighboring points around the center point, and g_c represents the center pixel. The function $s(x)$ is the central calculation function of LBP. When x is greater than or equal to 0, the value of $s(x)$ takes 1; otherwise, when x is less than 0, the value of $s(x)$ takes 0.

Based on the square LBP, the equivalent mode and the rotation invariance mode are derived. Both modes are defined on the basis of the circular mode. Taking the case

corresponding to the 3×3 square mode as an example, the circular mode is to draw a circle the radius of 1 outside the center pixel and evenly take 8 points passing through the circle as neighboring points. At this time, the point taken is likely not to pass through the center of the pixel, and interpolation must be used to estimate the coordinates of the pixel.

Considering that the LBP features obtained by different angles of image rotation are different, the rotation invariance mode cyclically shifts all the obtained 8-bit binary strings, and merges the histogram with the same minimum decimal value. The histogram thus obtained is 36-dimensional and is not affected by image rotation. The equivalent mode studies the hopping frequency of 0 and 1 in the bit string. It combines all the bit strings with hop times greater than 2 to obtain the 59-dimensional feature. These two modes reduce the dimensions on the square mode without losing too much valuable information.

The rotation invariant LBP we used can be defined as

$$LBP_{P,R}^{ri} = \min\{ROR(\sum_{p=0}^{P-1} s(g_p - g_c)2^p, P)\} \quad (5)$$

where $ROR(x,i)$ performs a circular bit-wise right shift on the x, i times, P represents the number of the adjacent points used around the center point, and R represents that the points used are on a circle of radius R.

In order to select the better features, we learned from the idea of Fisher score and defined the modified Fisher efficiency score on this basis. The main idea of the standard mode Fisher score is to calculate the ratio of the distances between classes to the inner-class distance. The higher the feature's score, the better the classification effect. However, for steganalysis, the LBP feature is affected by the image content. The traditional distances between classes calculation method cannot reflect the difference between the steganographic image set and the original image set. The distance between the steganographic image and the original image is used instead of the distance between the classes to better reflect the impact of steganography on the image. The modified Fisher score (MFS) we defined is shown as

$$\mathrm{MFS}(F) = \frac{d(F_s - F_c)}{\frac{1}{2}(d(F_s) - d(F_c))} \quad (6)$$

$$d(F_N^K) = \frac{\sum_{n=1}^{N}\sum_{k=1}^{K}(\mu_n^k - \mu^k)^2}{N} \quad (7)$$

where F_s represents the feature extracted from the steganographic images and F_c represents the feature extracted from the original images. $d(F_N^K)$ is a function for calculating the average distance of the vector group F_N^K. N is the number of vectors in the vector group and K is the dimension of the feature F_n. μ is the average vector of the vector group F_N^K.

The modified Fisher scores for the LBP features of different modes were calculated (A thousand grayscale images were selected from the BossBase1.0 image set as the experimental image set. This image set was used to test our algorithm parameters in the article).

The results obtained are shown in Tab. 3. Where re represents the square mode, eq represents the equivalent mode, ri represents the rotation invariance mode, and D represents the dimension of the feature vector in the mode.

Table 3: The modified Fisher score of the LBP algorithm in different modes

ratio=0.4	LSB	EA	HUGO	S-UNIWAARD	D
ri	1.9558	1.9563	1.9590	1.9588	36
eq	1.9650	1.9666	1.9698	1.9697	59
re	1.9699	1.9688	1.9736	1.9735	256

The experimental results show that the ri mode and eq mode scores are similar to the rec mode, but they have lower dimensions. In order to select the more efficient features based on maintaining good classification results, Eq. (8) is used to calculate the modified Fisher efficiency of the features. It can be seen in Fig. 3 that the ri mode has a higher modified Fisher efficiency when the revised Fisher score is similar. Therefore, in the subsequent research, the ri mode is apt to be used as the basic feature extraction mode.

$$\mathrm{MFE}(F_N^K) = \frac{\mathrm{MFS}(F_N^K)}{logK} \tag{8}$$

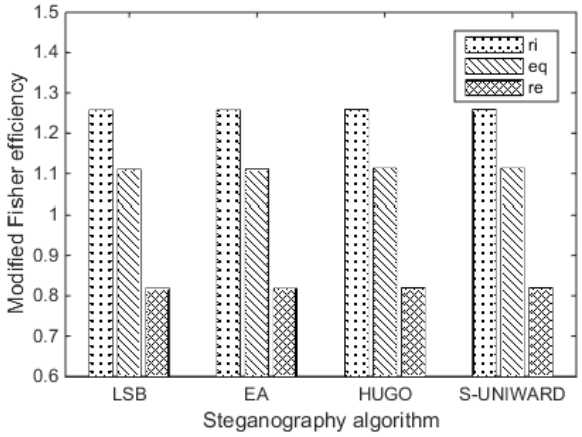

Figure 3: The comparison of different LBP basic modes

2.3 Design over LTP model

The detection accuracy of the LBP method cannot meet the requirements of steganalysis, so the improved method of the LBP, which is the LTP, is chosen. When the LSB or the LSBM algorithm embeds secret information, there will be three cases where the original pixel value is not changed, the original pixel value is incremented by one, and the original pixel value is decremented by one. However, the LBP can only detect two cases: the original pixel is incremented or not changed, and the original pixel value is decremented. To solve this problem, the LBP is extended to the LTP mode.

The LTP mode inherits different modes and parameters of the LBP. In the LTP mode, the

definition of the function $s'(x,t)$ is shown in Eq. (6). The 8-bit string thus obtained contains three different values of -1, 0, and 1. The portion with -1 and the portion with 1 should be taken apart before the bit string is decimal.

$$s'(x,t)=\begin{cases}1, x>+t,\\ 0, -t\le x\le +t,\\ -1, x<-t.\end{cases} \tag{9}$$

Taking the $LBP_{8,1}^{ri}$ mode as an example, after splitting, two sets of 8-bit binary strings will be obtained. The LBP algorithm is used to perform histogram statistics on two sets of binary strings, and each set of binary string will obtain a 36-dimensional feature vector. Combining the feature vectors obtained from the two sets of binary strings yields a 72-dimensional image feature vector, which is the LTP feature vector.

Compared to the LBP, the LTP mode has its own parameter t. In order to obtain a more accurate steganalysis result, the relevant parameters of the LTP are also optimized based on the appropriate LBP basic mode.

In order to test the effect of the parameter t on the performance of steganalysis, different values of parameters t are chosen for testing. Where t can take a single value of 0, 1, 2, or the combination of the different values of t. Tab. 4 shows the steganalysis error rates of the LTP with different t values. The payload we use is 0.4.

Table 4: Different steganography methods and LTP algorithm error rates under different parameters

ri, 0, 1	LBP	LTP (T=0)	LTP (T=0,1)	LTP (T=0,1,2)	LTP (T=1)	LTP (T=2)
LSBM	0.3080	0.2008	0.1334	0.0993	0.3667	0.3763
EA	0.4718	0.2303	0.1659	0.1313	0.1840	0.2443
HUGO	0.4947	0.4396	0.3924	0.3537	0.4148	0.4438
S-UNIWARD	0.4925	0.4414	0.4359	0.4186	0.4729	0.4857
D	36	72	144	216	72	72

When t takes a single value, the steganalysis error rate increases as the value of t increases. When t is 0, the error rate obtained is the lowest and lower than the error rate when using the LBP algorithm.

When the features of different values of t are used in combination, it can be seen that the more features of different values of t are used, the better the steganalysis performances. Generally, the higher the dimension of the feature vector, the better the classification result.

However, comparing the re mode to the LTP mode, the re mode has a higher dimension, but the low-dimensional LTP (t=0, 1, 2) mode has a lower error rate. Therefore, it can be concluded that the LTP has higher detection ability than the LBP for all the steganography methods given in the Tab. 4, and the detection capability for the LSBM is the best.

Base on the results in Tab. 4, the multi-mode is chosen to better reflect the relationship of the neighbor pixels:

$$msLTP = \left\{LTP_{P,R,t}^{ri} | R = \{1,2,3\}, t = \{0,1,2\}, P = 8\right\} \quad (10)$$

2.4 The msdeLTP model

Based on the previous research on the LTP feature extraction algorithm and derivative filter, this paper combines the two improvements. A derivative filter is introduced in the process of generating a residual image, and the LTP algorithm is used to extract features. The steganalysis system based on the LTP and derivative filter thus obtained is called the deLTP steganalysis system. The simulation results are shown in Fig. 4.

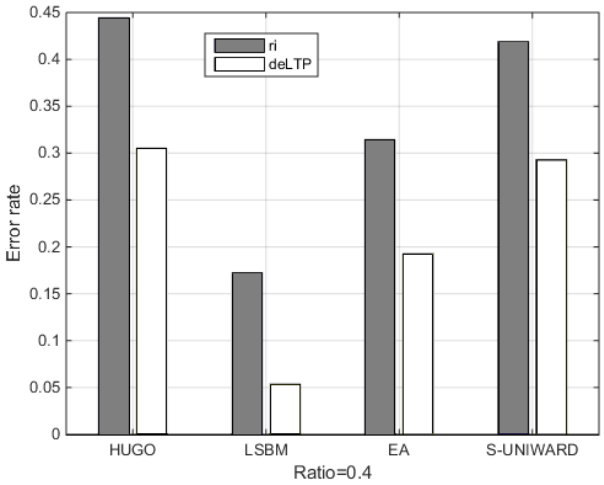

Figure 4: Error rate comparison between deLTP-based steganalysis system and LBP-based steganalysis system

In Fig. 4, the deLTP is compared with the common LBP algorithm. It is found that in the case of the same steganography rate, the error rate obtained by the test based on the deLTP steganalysis system is greatly reduced for both the image adaptive steganography algorithm and the non-image adaptive steganography algorithm.

The msdeLTP model we ultimately use is a combination of multi-scale LTP features based on the deLTP, that is, the combination of feature data in different neighborhoods. The multi-scale mode enables the feature vector to better consider pixel variations in different neighborhoods, and can further reduce the error rate of the detection algorithm based on the deLTP algorithm. Here we use 3×3, 5×5 and 7×7 neighborhoods, that is, take the radius r as 1, 2, 3, and the basic mode uses ri mode, so that the eigenvector is 2592. The steganalysis model in this case is referred to as the msdeLTP model.

The msdeLTP uses derivative filters to extract the residual images before extracting the features, because the residual images better reflect the characteristics of the steganographic image compared to the image itself. Based on the standard LBP, the msdeLTP uses the rotation invariance mode to further reduce the dimension of the LBP

feature while the information is still contained in the features. At the same time, in order to better detect the texture information of the image, the msdeLTP uses the multi-scale LTP mode. The algorithm uses a combination of multiple t values to ensure the sensitivity of the algorithm. The optimized msdeLTP has 2592 features, which is one tenth of the number of the SRM features. Although the msdeLTP has fewer features, it still maintains good detection accuracy.

The msdeLTP model we propose can be defined as

$$msdeLTP = \left\{ LTP_{P,R,t}^{ri}(\boldsymbol{P} * \boldsymbol{C3}) | r = \{1,2,3\}, t = \{0,1,2\}, P = 8 \right\} \quad (11)$$

where $\boldsymbol{P}$ represents the carrier image, $\boldsymbol{C3}$ represents the derivative filter bank we selected above, and the residual image group of $\boldsymbol{P}$ is obtained by the operation $\boldsymbol{P} * \boldsymbol{C3}$.

3 Simulation results and analysis

In order to verify the performance of the steganalysis algorithm, four steganography methods were chosen as the detected objects, namely LSB, EA, S-UNIWARD and HUGO. 10000 test images were from BOSSBase1.01. The ensemble classifiers in 5-fold cross validation mode were used to classify the extracted features. For each set of data, we performed the same experiment five times and averaged the experimental results to ensure the reliability of the results.

Fig. 5 shows the detection error rate of the msdeLTP for different steganography algorithms under different payloads. It can be seen that the msdeLTP performs well for different algorithms including adaptive steganography.

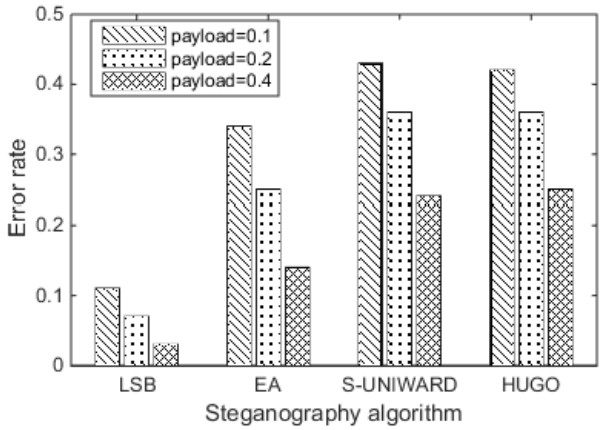

Figure 5: The error rates of different steganography algorithms

A comparison of the steganalysis error rates for the msdeLTP and the SRM algorithms is shown in Fig. 6. In the same situation, the error rate of the msdeLTP is close to that of the SRM, while the feature dimension of the msdeLTP is 2592, which is only one tenth of the SRM. Therefore, the msdeLTP maintains good efficiency.

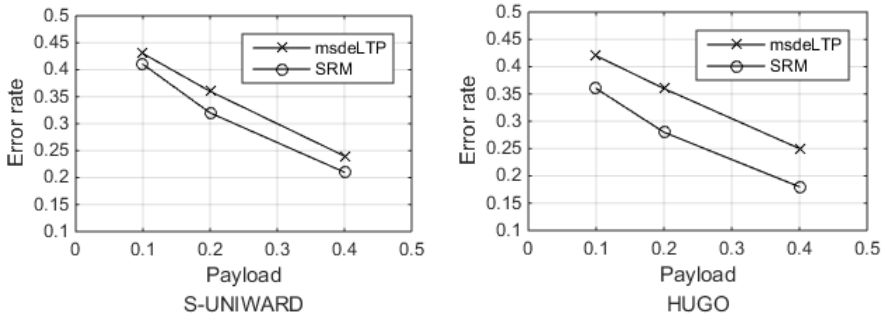

Figure 6: Performance comparison of the msdeLTP and the SRM

4 Conclusion

The LBP based methods have good prospects in steganalysis, but existing detection algorithms can only detect the LSBM algorithms and cannot be applied to other steganography algorithms. Based on the LBP methods, in order to reduce the impact of image content on steganalysis, the msdeLTP uses derivative filters to obtain the residual images. The msdeLTP extracts features on the residual images, suppressing the original image noise and improving the detection performance of the steganalysis. In addition, the msdeLTP uses a multi-scale LTP mode that reflects changes in pixels over a larger area. The msdeLTP can achieve similar detection accuracy as the SRM. At the same time, compared with the SRM, the msdeLTP has smaller feature sizes and lower time complexity, which means features can be extracted with a faster speed. Compared with other LBP based methods, the msdeLTP guarantees the accuracy of detection and extends the scope of steganography algorithms can be detected.

Our future research will focus on combining the characteristics of adaptive steganography algorithms into the msdeLTP, such as giving higher weights to image texture regions, and giving lower weights to smooth regions, to help the proposed algorithm detect adaptive steganography algorithm better.

Acknowledgement: This work is supported by Major Scientific and Technological Special Project of Guizhou Province (20183001), Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ014), Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ019) and Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2018BDKFJJ022).

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

References

Denemark, T.; Sedighi, V.; Holub, V.; Cogranne, R.; Fridrich, J. (2014): Selection-channel-aware rich model for steganalysis of digital images. *IEEE International Workshop on Information Forensics and Security*, pp. 48-53.

Fridrich, J.; Kodovsky, J. (2012): Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics & Security*, vol. 7, no. 3, pp. 868-882.

Goljan, M.; Fridrich, J.; Cogranne, R. (2014): Rich model for steganalysis of color images. *IEEE International Workshop on Information Forensics and Security*, pp. 185-190.

Gui, X.; Li, X.; Yang, B. (2014): Steganalysis of LSB matching based on local binary patterns. *Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 475-480.

Holub, V.; Fridrich, J. (2013): Random projections of residuals for digital image steganalysis. *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1996-2006.

Kodovsky, J.; Fridrich, J. (2012): Steganalysis of JPEG images using rich models. *Media Watermarking, Security, and Forensics*, vol. 8303.

Lei, M.; Yang, Y. X.; Niu, X. X.; Yang, Y.; Hao, J. (2017): An overview of general theory of security. *China Communications*, vol. 14, no. 7, pp. 1-10.

Lin, Q.; Liu, J.; Guo, Z. (2016): Local ternary pattern based on path integral for steganalysis. *IEEE International Conference on Image Processing*, pp. 2737-2741.

Lafferty, P.; Ahmed, F. (2004): Texture-based steganalysis: results for color images. *Proceedings of SPIE*, vol. 5561, pp. 145-151.

Ojala, T.; Pietikäinen, M.; Harwood, D. (1996): A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*, vol. 29, no. 1, pp. 51-59.

Ojala, T.; Pietikäinen, M.; Maenpaa, T. (2002): Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Madchine Intelligence*, vol. 24, no. 7, pp. 971-987.

Shi, Y. Q.; Sutthiwan, P.; Chen, L. (2012): Textural features for steganalysis. *International Workshop on Information Hiding*, vol. 7692, pp. 63-77.

Tan, X.; Triggs, B. (2010): Enhanced local texture feature sets for face recognition under difficult lighting conditions. *IEEE Transactions on Image Processing*, vol. 19, no. 6, pp. 1635-1650.

Tang, W.; Li, H.; Luo, W.; Huang, J. (2016): Adaptive steganalysis based on embedding probabilities of pixels. *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 4, pp. 734-745.

Yang, Y.; Chen, Y. W., Chen, Y. L.; Bi, W. (2018): A novel universal steganalysis algorithm based on the IQM and the SRM. *Computers, Materials & Continua*, vol. 56, no. 2, pp. 261-272.