International Conference on Precision Machining, Non-Traditional Machining and Intelligent Manufacturing (PNTIM 2019)

Research on Image Steganography Information Detection Based on Support Vector Machine

Wenyuan Liu
School of Information Science and Engineering
Yanshan University
Qinhuangdao Hebei, 066004, China
E-mail: robertwang0499@163.com

Jian Wang*
School of Information Science and Engineering
Yanshan University
Qinhuangdao Hebei, 066004 China

***Abstract*—With the rapid development of the internet of things and cloud computing, users can instantly transmit a large amount of data to various fields, with the development of communication technology providing convenience for people's life, information security is becoming more and more important. Therefore, it is of great significance to study the technology of image hiding information detection. This paper mainly uses the support vector machine learning algorithm to detect the hidden information of the image, based on a standard image library, randomly selecting images for embedding secret information. According to the bit-plane correlation and the gradient energy change of a single bit-plane after encryption of an image LSB matching algorithm, gradient energy change is selected as characteristic change, and the gradient energy change is innovatively applied to a support vector machine classifier algorithm, And has very good detection effect and good stability on the dense image with the embedding rate of more than 40 percent.**

Keywords-Support Vector Machine; Information Detection; LSB Matching; Steganography

I. INTRODUCTION

Information detection technology has developed with the birth of information hiding technology. Different countries use different technologies to hide secret information. Since the 1990s, with the rapid development of the internet and information multimedia technology, the technology of steganography of secret information into multimedia has gradually become a hot research topic for scientists and technicians [1]. At the same time, the detection technology of hidden information has gradually become a key research direction in this period. Steganography technology can be used to do secret information transmission; can serve the people's privacy very well. but with the development of encryption technology and detection technology, information hiding methods are used by criminals to do harm to public security, which poses a threat to human life safety. Such as an auction site used by spies to pass confidential information [2], therefore, it is very important to study the hidden information detection technology. Nowadays, image is the main way to spread secret information. Because of its redundancy and sufficient space, it is best to use image as the carrier of secret information. The main research methods of image hiding technology include LSB matching [3] , outguess [4], F5[5] and so on.

II. SUPPORT VECTOR MACHINE CLASSIFICATION ALGORITHMS

Hypothetical training sample $\{(x_i, y_i), i = 1, 2, \cdots, l\}$, Where $x_i \in R^d$ is that input vector of the $i'th$ d - dimensional column, $y_i \in R$ is the output that matches. The high-dimensional mapping method based on support vector machine (SVM) can be transformed into a linear problem [6], and then a linear classification model is established.

$$f(x) = \{w, \varphi(x)\} + b \tag{1}$$

Mapping the standard line of this model to a high-dimensional space can be called the optimal hyperplane; from the two-dimensional calculation formula we can get the following extensions, there is a value i that satisfies $y_i = 1$

$$(\omega \cdot x_i) + b \geq 1 \tag{2}$$

There is a value i that satisfies $y_i = -1$

$$(\omega \cdot x_i) + b \leq -1 \tag{3}$$

Combined formula (2) and (3), there are

$$y_i((\omega \cdot x_i) + b) \geq 1, i = 1, 2, \ldots l \tag{4}$$

$\|\omega\| / 2$ has the minimum value which is $2/\|\omega\|$ largest. So according to the duality theory can be converted into:

$$\min_{w,b} 1/2\|\omega\|^2 \; s.t - y_i((\omega \cdot x_i) + b) \geq 1, i = 1, 2, \ldots l \tag{5}$$

Equation (5) is obviously a quadratic convex programming problem. In order to solve this problem, Lagrange operator is introduced to solve the problem. By adding auxiliary variable Lagrange operator, constrained programming is transformed into unconstrained optimization

problem. The Lagrange operator used here is noted as: $\alpha = (\alpha_1, \ldots, \alpha_l)^T \in R_+^l$, So there are:

$$L(\omega, b, \alpha) = \frac{1}{2}\|\omega\|^2 - \sum_{i=1}^{l} \alpha_i (y_i((\omega \cdot x_i) + b) - 1) \quad (6)$$

Here will minimize the risk as a conditional extremum algorithm, on the premise of duality theory, assuming that the conditional extremum is $\nabla_b L(\omega, b, \partial) = 0$ and $\nabla_\omega L(\omega, b, \alpha) = 0$, there are:

$$\sum_{i=1}^{l} y_i \alpha_i = 0 \quad (7)$$

$$\omega = \sum_{i=1}^{l} \alpha_i y_i x_i. \quad (8)$$

According to the duality theory are:

$$\min_{\alpha} \frac{1}{2} \sum_{i=1}^{l} \sum_{j=1}^{l} y_i y_j \alpha_i \alpha_j (x_i \cdot x_j) - \sum_{j=1}^{l} \alpha_j$$

$$s.t. \sum_{i=1}^{l} y_i \alpha_i = 0 \quad \alpha_i \geq 0, \ i = 1, \ldots, \ l \quad (9)$$

Equation (9) is an inequality constrained quadratic programming, according to the principle of optimization, to get the optimal solution of (9), must meet the following conditions:

$$\alpha_i \{ y_i [(\omega \cdot x_i) + b] - 1 \} = 0, \ i = 1, 2, \ldots, \ l \quad (10)$$

After adding optimization conditions for learning training, and then the main factor in such a data set is the so-called support vector, they close to the edge of each classification point, if the data is removed, classification surface is the same, the support vector to get the most results $\alpha^* = (\alpha_1^*, \ldots, \ \alpha_l^*)^T$. The end result is $\omega^* = \sum y_i \alpha_i^* x_i$, α_j^* data a extracted here is classified as α^*, and the final result is

$$b^* = y_j - \sum y_i \alpha_i^* (x_i, x_j) \quad (11)$$

The type of support vector machine algorithm optimization problem is transformed into linear equations. the final classification model is:

$$f(x) = \operatorname{sgn}\left(\sum_{i=1}^{l} \alpha_i^* y_i (x \cdot x_i) + b^* \right) \quad (12)$$

In equation (12), $y_i(x \cdot x_i)$ is a kernel function satisfying the Mercer condition. When the form of the nonlinear transformation algorithm is not clear, the kernel function can solve the basic nonlinear problem, but it is also an obvious feature of the support vector machine algorithm.

III. MULTI-FEATURE DETECTION CLASSIFICATION MODEL BASED ON SUPPORT VECTOR MACHINE

Multi-feature detection technology is a general-purpose detection technology, which is a common means of steganography detection. The direct purpose of multi-feature detection is to distinguish between the original image and the image containing secret information, so as to further process the image containing secret information. According to the support vector machine classifier, the original image and the steganography image are classified with the minimum error probability, and this classification belongs to the case of two classifications.

A. Bit plane correlation

In the image, there are two vectors, vector v and vector w, and the linear correlation relationship between them is represented by the following [7]

$$z(v, w) = \frac{1}{N} \sum_{i} v[i] \times w[i] \quad (13)$$

In equation (13), N is the number of subsets contained in the vector. In the field of communication, a predetermined threshold value of two new signals and a linear relationship between the two signals are usually used as a judgment for detecting whether there is noise between the two signals that is, detecting whether a mixed signal occurs therein[8]. For digital images, the image has several planes and can be said to have several signals, so that the image can calculate the linear relationship between several signals to check whether the image has steganography information.

B. Potential plane gradient energy variation

Gradient energy is an element that can effectively measure image pixel correlation, and in one-dimensional cases, the gradient can be represented by equation [14]

$$r(n) = I(n) - I(n-1) \quad (14)$$

Then one-dimensional gradient energy can be expressed as follows:

$$GE = \sum |I(n) - I(n-1)|^2 = \sum |r(n)|^2 \quad (15)$$

In formula (15), I is a pixel value, the larger the gradient energy, the smaller the correlation between the pixels. When LSB replacement steganography is used in image information, the correlation between the lowest bit pixels will be weakened and the gradient energy will be greatly enhanced. After LSB matching steganography, all bit planes of the image will fluctuate, so the gradient energy cannot completely show the change of bit planes, so after LSB matching algorithm steganography gradient energy can be expressed as:

$$GE_i = \sum \left(I_i(n) - I_i(n-1) \right)^2 \quad (16)$$

In equation (16), GE_i represents the gradient energy of the i bit plane, and I_i represents the value of the i bit plane of the pixel.

In the same way, the feasibility of using GE_i as eigenvalue is analyzed effectively. After the standard image is matched by LSB, secret information is embedded with embedding rates of 0 %, 30 %, 50 %, 80 % and 100 % respectively; the change in gradient energy in the image is shown in table 1

TABLE I. GRADIENT ENERGY VARIATION OF LOWER SURFACE WITH DIFFERENT EMBEDDING RATES

Embedding rate	Bit area 5	Bit area 6	Bit area 7	Bit area 8
0%	1.98111	4.67108	1.16220	2.28016
30%	1.99201	4.68920	1.16523	2.28639
50%	2.00200	4.70426	1.16990	2.30474
80%	2.01137	4.72238	1.17129	2.30146
100%	2.01723	4.76232	1.17883	2.32047

From the above description, in the process of detecting the image, the correlation of the 7 and 8 planes of the image can be compared with the gradient energy of the other bit planes, and finally the feature vectors $F = [F1, F2, F3, F4, F5, F6, F7, F8, F9]$ can be obtained. In this paper, support vector machine is used as classifier. The kernel function chooses linear kernel function. The flow chart of the final detection is shown in Figure 1.

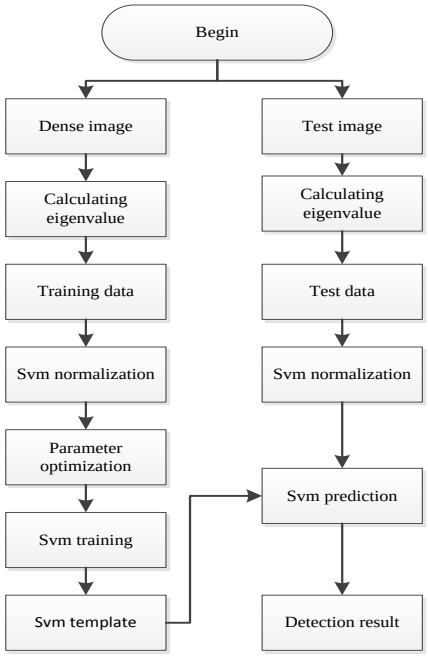

Figure 1. SVM classifier detection process

C. Correlation formula

In this paper, there are four kinds of detection standards used in the process of image support vector machine detection, they are detection rate, miss rate, false alarm rate and real rate [41 - 43], and their calculation method is as follows:

$$TPR = TP / (TP + FN) \quad (17)$$

$$FNR = FN / (TP + FN) \quad (18)$$

$$FPR = FP / (FP + TN) \quad (19)$$

$$DR = (TP + TN) / (TP + FP + TN + FN) \quad (20)$$

The parameters involved in equations (17), (18), (19), (20) are defined as follows (The dense image is a positive sample and the original image is a negative sample): *TP* is the sum of the number of positive samples whose prediction results are all positive; *FP* is the sum of the number of positive samples whose prediction results are negative; *TN* is the sum of the number of negative samples whose prediction results are negative; *FN* is the sum of the number of positive samples whose prediction results are negative; *TPR* is the percentage of positive samples whose predictions are negative; *FPR* is the percentage of positive samples (false alarm rate) where the prediction results are negative; *FNR* is the percentage of negative samples whose prediction results are negative (miss rate); *DR* is the percentage of positive samples whose predictions are negative

After the support vector machine detection and classification, the percentage of the correct detection of the dense image is called the true rate, the percentage of errors in the detection of dense image is called the miss rate, the percentage of errors in the detection of the original image is called the false alarm rate, from the overall point of view, the original image and the dense image detection results are consistent with the percentage of the real image is called the detection rate.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental conditions

Simulation environment of this paper: MATLAB 2014a. In this experiment, NRCS uncompressed image library is used as the experimental image library source, images are downloaded randomly from the original image library; they are all converted to BMP image format in some way and the final image is cropped to 610 x 418 sizes. The center point of the image is still processed around the center point of the original image. Finally, the standard algorithm is used to transform all images into 8 - bit gray images.

In this paper, the image embedding rate is calculated as follows: 100 % embedding rate refers to all the pixels of the image for steganography, 90 % refers to every 10 pixels of all the images for steganography 9 and then the remaining one to continue, the other embedding rate in turn and so on.

Generation of steganography image: after the original image is processed, the 8 - bit gray image is encrypted by MD5 encryption algorithm, then the encrypted information is embedded into the image by LSB matching algorithm, and different steganography images are obtained according to different embedding rates.

B. Experimental process and result analysis

In order to better test the experimental results, this paper adopts two kinds of test methods in the process of image steganography detection. Individual test is that only one embedding rate of encrypt images in all test samples; Hybrid testing means that the embedding rate of encrypted images in all test samples is mixed[9]. The main purpose of those two tests is to estimate the embedding rate limit of the detection effect and to measure the stability of the detection algorithm.

1) Individual test

200 images are randomly selected from the processed 8 - bit grayscale images to be labeled S1, and 200 images different from S1 are randomly selected to be labeled S2. The specific treatment process is as follows.

Step1 200 steganography images with an embedding rate of 10 % are generated by S1, and 400 images in total are added by S1 to serve as a training sample set of the support vector machine classification algorithm.

Step2 1,000 steganography images with an embedding rate of 10 % generated by S2 are added with a total of 1,200 images generated by S2 to serve as a test sample set of the support vector machine classification algorithm.

Step3 the eigenvalues of the two samples are calculated respectively according to the method used in the previous section, and finally displayed in the format of a data file.

Step4 normalizing the data file to obtain a legal machine input file.

Step5 parameters *C* and *G* were determined by cross-validation method

Step6 the prediction samples are classified and predicted by using support vector machine.

Step7 the embedding rates are 20 %, 30 %, 40 %, 50 %, 60 %, 70 %, 80 %, 90 %, 100 % respectively, and then the processes of (1) to (6) are repeated. Table 2 shows the selection of optimal parameters for cross-validation of support vector machines with different embedding rates.

TABLE II. BEST PARAMETERS FOR TRAINING TEMPLATES

Embedding rate	*C*	*G*
100%	2.0	0.5
90%	2048.0	0.03125
80%	8192.0	0.0078125
70%	2048.0	0.03125
60%	512.0	0.03125
50%	32768.0	0.001953125
40%	32768.0	0.0078125
30%	32768.0	0.0078125
20%	32.0	0.00048828125
10%	512.0	0.0001220703125

TABLE III. IMAGE TEST RESULTS

Embedding rate	Detection rate	Missing rate	False alarm rate
100%	95.7%	1.2%	7.4%
90%	95.15%	5.9%	3.8%
80%	93.85%	7.2%	5.1%
70%	93.4%	5.9%	7.3%
60%	87.35%	9.4%	15.9%
50%	73.35%	35.4%	17.9%
40%	83.65%	12.2%	20.5%
30%	57.7%	60.6%	24%
20%	50.9%	2.9%	95.3%
10%	50.65%	3.3%	95.4%

As can be seen from Table 3, when the image embedding rate gradually decreases, the detection rate of the image also decreases, and the trend of the embedding rate and the detection rate conforms to the current theoretical information. When the embedding rate is greater than or equal to 40 %, the detection rate of the image is above 80%; When the embedding rate is greater than or equal to 70 %, the detection rate of the image is more than 90 %, and when the embedding rate is less than or equal to 30 %, the detection rate of the image is about 50 %. Therefore, the support vector machine detection method is suitable for dense image detection with high embedding rate.

2) Hybrid test

In the experiment, two different combination methods are used to combine the test samples。Firstly, the combination of keeping the number of samples tested constant and just grouping the samples tested into groups every two shows that image changes do not affect the stability of SVM; Secondly, The test samples are combined freely in order from less to more, so that the test samples of the sample set are more and more. The combination of this means may illustrate that when the number of images is large, the stability of the support vector machine algorithm itself is not unstable because of the number of images.

In the experimental process, the first case is tested to keep the number of test samples unchanged while ensuring that the contents of the two sample images are inconsistent. 200 original images are randomly selected, and another 200 original images are encrypted by MD5 encryption algorithm using LSB matching algorithm to form a steganography image. This takes the original image together with the encrypted image as a training sample for the support vector machine classifier. The test sample is divided into five parts; each part selects 300 randomly selected original images for MD5 encryption algorithm. This test sample set and training sample set a total of 1900 pieces, the data together to support vector machine training and prediction, the final prediction results are shown in Figure 2

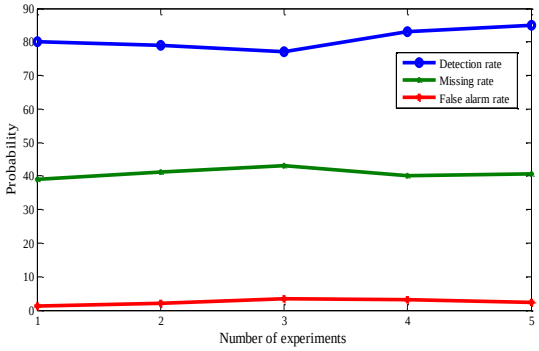

Figure 2. Algorithm stability test results one

As can be seen from fig.2, the final detection rate of the combination of five parts and two parts is about 80 %, the missed detection rate is about 40 %, the false alarm rate is controlled below 10 %, and the corresponding curve of the image fluctuates little. Therefore, the image changes will not affect the stability of support vector machine, so the algorithm has a good practical application value.

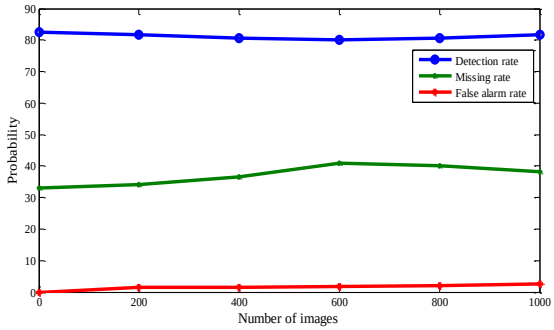

Figure 3. Algorithm stability test results two

Then, the second case is tested, 300 original images are randomly selected, and another 300 original images are encrypted by MD5 encryption algorithm using LSB matching algorithm to form a steganography image (The embedding rate is 50 %, 80 % and 100 % respectively), a total of 600 original image and encrypted image of that training sample were recorded. The test sample was divided into six parts, the original image samples for each portion are combined using images grouped into 30, 60, 120, 240, 480, and 960 respectively, and the number of the steganography images of each part is kept equal to the number of the original images, while ensuring that the embedding rate of 50 %, 80 % and 100 % is equal to the proportion of the encrypted images. The data are fed into a support vector machine for training and prediction, and the final prediction result is shown in Fig.3.

As can be seen from fig. 3, the detection rate of the six-part size combination is about 80 %, the missed detection rate is about 40 %, the false alarm rate is controlled below 5 %, and the corresponding curve of the image fluctuates little, so the image change does not affect the stability of the support vector machine, so the algorithm has good practical application value.

V. CONCLUSIONS

According to the bit-plane correlation and the gradient energy change of a single bit-plane after encryption by an image LSB matching algorithm, according to the change of the feature quantity, a support vector machine classifier algorithm is applied to detect the encrypted image, The method has good detection effect and good stability on a dense image with an embedding rate of more than 40 %. It provides a good method for the detection of the hidden writing of images

REFERENCES

[1] Fridrich J, Du R. Secure steganographic methods for palette images [C]//International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 1999: 47-60..

[2] Cheddad A, Condell J, Curran K, et al. Digital image steganography: Survey and analysis of current methods[J]. Signal processing, 2010, 90(3): 727-752.

[3] Juarez-Sandoval O, Cedillo-Hernandez M, Sanchez-Perez G, et al. Compact image steganalysis for LSB-matching steganography [C]//Biometrics and Forensics (IWBF), 2017 5th International Workshop on. IEEE, 2017: 1-6.

[4] Chhikara R R, Kumari M. Significance of feature selection for image steganalysis[C]//Computation System and Information Technology for Sustainable Solutions (CSITSS), International Conference on. IEEE, 2016: 75-79.

[5] Fridrich J, Goljan M, Hogea D. Steganalysis of JPEG images: Breaking the F5 algorithm[C]//International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 2002: 310-323.

[6] Kim K I, Jung K, Kim J H. Texture-based approach for text detection in images using support vector machines and continuously adaptive mean shift algorithm[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(12): 1631-1639.

[7] Pan B, Qian K, Xie H, et al. Two-dimensional digital image correlation for in-plane displacement and strain measurement: a review[J]. Measurement science and technology, 2009, 20(6): 062001.

[8] Zhi L, Fen S A. Detection of random LSB image steganography [C]//Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. IEEE, 2004, 3: 2113-2117.

[9] Wang X, Liu Q, Wang R, et al. Natural image statistics based 3D reduced reference image quality assessment in contourlet domain[J]. Neurocomputing, 2015, 151: 683-691.