Key Technical Analysis on Steganography and Steganalysis

Huayong Ge , Hongqiang Liu and Zhaoyang Jin

Abstract. In this paper, we present F5 steganographic algorithm and its steganographic system, then we embed 35.5kb information (a txt document) into a 99.7kb JPEG image by using F5 steganographic system. The experimental result shows that when we choose k=3 which is based on utilization rate of the data(R), then the AC coefficients will be changed seldom while the information embedded in the image. The three domains method to steganalysis the stego-images is also analyzed in this paper. Extracting the three domains characteristics on the JPEG images to train the BP neural network classifier, we can set a threshold value to the BP neural network classifier to classify the JPEG images. The experimental results show the method using three domains offers a high accuracy to detect the image whether includes information or not.

Keyword: F5 stegaographic algorithm • steganographic system • matrix encoding • the BP neural network classifier

1 Introduction

In the 1990's, with the development of computer technology, steganography and steganalysis technology developed quickly [1]. Because JPEG image has the advantages of high compression ratio, it becomes the Internet's most popular image format. The research on steganography in the DCT (Discrete Cosine Transform) domain is a hot issue in present study [2]. At the same time, the steganalysis technology in JPEG image is also continuously developing.

DCT transform is one of the important technologies in JPEG compression technology. At the beginning, JSteg[3] was a common steganography method, but this method can cause the change of AC (Alternating Current) coefficient histogram, and it will make us find the presence of steganographic information easily while using Chi-square test. With the continuous development of steganographic

[1] Huayong Ge(✉)

1) College of Information Sciences and Technology

2) Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education

DonghuaUniversity, Shanghai 201620, P. R. China

e-mail: gehuayong@dhu.edu.cn

[2] Hongqiang Liu(✉)

1) College of Information Sciences and Technology

2) Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education

DonghuaUniversity, Shanghai 201620, P. R. China

e-mail: liuhongqiang@126.com

techniques, OutGuess [4] and F5 [5] steganographic methods appeared.

There are two ways of steganalysis in JPEG image: specific steganalysis and general steganalysis [6]. Specific steganalysis is usually used for the known steganographic methods, while general steganalysis is used for the steganographic methods which are not known. The methods of general steganalysis can be divided into three steps: estimation of the steganographic information, feature extraction and classification.

In the rest of this paper, section II illustrates the principle of F5 algorithm, and uses F5 steganographic system to experiment with the JPEG images. When we choose the relevant k-value which is equal to utilization rate of the data, we can see the AC coefficients changed little by embedding a 35.5kb txt document into a 99.7kb JPEG image. Section III describes the principle of three domains characteristics of the blind detection, and we extract the three domains characteristics of JPEG images to train the BP neural network classifier. Then, we classify the stego-images by setting the threshold value. Experiment result shows that three domains method would make you get a high accuracy. Concluding remakes are given in section IV.

2 Analysis to the F5 algorithm

There are a lot of steganography algorithms based on DCT domain in the JPEG images. Among them F5 algorithm is an important steganographic algorithm. It is based on the F4 steganographic algorithm, and introduces the shuffle and matrix coding technology. With both of these technologies, F5 algorithm makes steganographic image quality equalization, and improves the embedding efficiency.

Compared with F4, F5 breaks the order of JPEG image's DCT coefficient, and gets a new DCT coefficient sequence. After that, we can embed the secret information in the new DCT coefficients. This is the shuffle technology which F5 algorithm used to improve the equilibrium level of the image. Besides using the shuffle technology, F5 algorithm has used the matrix coding technology. Using the matrix coding technology, F5 improves the embedded efficiency greatly. The basic idea of matrix coding method is to use n bits of LSB to represent k bit information $(n > k)$. For example, if we want to embed two bits $(x1, x2)$ among three bits $(a1, a2, a3)$ in LSB, we can change only one bit in LSB to represent the two bits. There are four kinds of cases will appear:

Case1: $x1 = a1 \oplus a3, x2 = a2 \oplus a3$ change nothing

Case2: $x1 \neq a1 \oplus a3, x2 = a2 \oplus a3$ change a1

Case3: $x1 = a1 \oplus a3, x2 \neq a2 \oplus a3$ change a2

Case4: $x1 \neq a1 \oplus a3, x2 \neq a2 \oplus a3$ change a3.

Here, the symbol' $\oplus$ 'represents XOR. In these four situations, the change is not more than one bit.

We can have a hypothesis that $n\ (n = 2^k - 1)$ original LSB bits are made to load k bits secret information, and we just change only one bit of them. We can record it as $(1, n, k)$. The embedding

efficiency: $E=\frac{2^k}{2^k-1}k$, the change density: $D=\frac{1}{n+1}=\frac{1}{2^k}$, the embedding rate: $R=\frac{k}{2^k-1}$ $(R\ll 1)$. It can be seen that the utilization rate of carrier reduced after using the matrix coding technology.

For using different matrix coding way, the relation among the change density, embedding rate and embedding efficiency is shown in table 1.

Table 1 Connection between change density and embedding rate

k	n	D	R	E
1	1	50.00%	100%	2
2	3	25.00%	66.67%	2.67
3	7	12.50%	42.86%	3.43
4	15	6.25%	26.67%	4.27
5	31	3.12%	16.13%	5.16
6	63	1.56%	9.52%	6.09
7	127	0.78%	5.51%	7.06
8	255	0.39%	3.14%	8.03
9	511	0.20%	1.76%	9.02

We use F5 steganographic system to embed 35.5 kb information into a JPEG image which is 99.7kb. The images before and after embedded are showed in Figure1 and Figure3, and the 35.5kb information is a TXT document which is shown in Figure 2.

Fig.1 Image Before Using F5

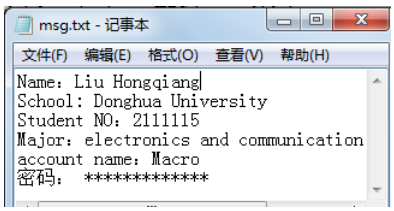

Fig.2 Msg.txt

Fig.3 Image After Using F5

Here the utilization rate of the data: $R=35.5kb/99.7kb=35.6\%$, and R is between the values when $k=3$ and $k=4$. For the table 1, when we choose $k=3$, we could embed $(99.7kb/7)*8=113.9kb$ information while we may embed $(99.7kb/15)*8=53.2kb$ information if we choose $k=4$. Here we should choose $k=3$ because we could embed larger

information than that we choose $k = 4$. The results show that we used $(1, 7, 3)$ coding mode, and 17057 coefficients changed (efficiency: 4.1 bits per change).

The result shows that the F5 algorithm offers a large steganographic capacity and improves the efficiency of embedding.

3 Analysis to the blind detection of three domains

General steganalysis is also called blind detection, and it is a method to detect the images of which have steganography in an unknown way and judge whether it contains hidden information or not. At present, there are several classical blind detecting methods. For example, Farid [7] proposed a blind detection method based on wavelet coefficient PDF moment [8], and Harmsen [9] proposed a method based on the histogram characteristic function centroid. However the blind detect methods above usually used the single characteristic to detect the image, the accuracy is low.

Luo put forward a blind detection method by three domains characteristics. The three domains characteristics are spatial domain characteristics, DCT domain characteristics and wavelet domain characteristics. First, we should extract the three domain characteristics. After extracting the characteristics, we could detect the JPEG image by the BP neural network classifier. The basic ideas of extract ing the three domains characteristics showed as follows.

3.1 Spatial domain characteristics extraction

We use $s_1, s_2, \cdots, s_N$ to represent image pixel values (the subscript is the index of the sample in the image), and one sample would be recorded as (s_i, s_j), and $1 \le i, j \le N$. We record P as a sample extracted from the image, and it can be regarded as a multiset [10] which is consisted by a series of two-tuples (u, v). Here the u and v are adjacent pixels, $0 \le u \le 2^b - 1$, $0 \le v \le 2^b - 1$, and the b represents the bits of each sample. It will exist 2 multisets: X_{2m+1} and Y_{2m+1}. Both of them have the sample (u, v), and $|u - v| = 2m + 1$, here $m = 0, 1, 2, \cdots, 127$. For natural images, the odd-even probabilities of the larger pixel values are the same while the digital sum variation is $2m+1$. After we embed information in the image, the situation will change. We look the deviation degree of multiset (X_{2m+1} and Y_{2m+1}) when $m = 0$ as spatial characteristics, and recorded it as $\delta = \dfrac{\big||Y_1| - |X_1|\big|}{|Y_1| + |X_1|}$.

3.2 DCT domain characteristics extraction

It is known that block of DCT coefficient obey Gaussian distribution, and each one of these macro

blocks is composed by four connected pieces which have small 8×8 pieces. Before and after embedding the information the variance of the scale parameter which obeys Gaussian distribution will change, so we can select parameters variance as characteristics.

1. For the images of each macro block，calculating the Laplacian parameters $\hat{\lambda}_i$. All the macro block Laplacian parameter vector could be recorded as $\hat{\lambda}=\{\hat{\lambda}_1,\hat{\lambda}_2,\cdots\hat{\lambda}_L\}$, and the '$L$' stand for blocks of the image macro block.

2. Calculating the average value of the Laplacian parameters in image: $\bar{\lambda}^h=(1/L)\sum_{i=1}^{L}\hat{\lambda}_i$ .And its variance is: $Var[\lambda^h]=(1/(L-1))\sum_{i=1}^{L}(\hat{\lambda}_i=\bar{\lambda}^h)^2$

According to step 2，we can get the characteristic value in DCT domain : $Var[\lambda^h]$.

3.3 Wavelet domain characteristics extraction

First of all, we do Haar wavelet decomposition to JPEG image. Then, extracting fourth order matrices from the 6 high frequency sub-band coefficient which is got decomposed. The four order matrices (average value, variance, skewness, peak) are looked as wavelet domain characteristics. In total, there are 24 characteristics, and we can call them F_{DWT} .

At last, we can classify characteristics and judge the JPEG images whether hide information or not by using the BP neural network classifier.

In the experiment, we detect the accurate rate of the steganalysis by three domains characteristics. First, we choose 1000 JPEG images from my own photos, and do steganography to all of them by four different steganography methods (JPhide, F5, MB, OutGuess). After steganography, we could get 2000 JPEG images (the original images and steganography images). Then, we train the BP neural network classifier by the 1500 JPEG images and set the threshold value to the classifier which has been trained.At last, we use the 500 JPEG images which are not trained to judge the images hide information whether or not by the method of three domains characteristics. The accuracy of steganalysis showed on Table II.

Table 2. the accuracy of steganalysis on the JPEG images

Threshold Value	**Method of two domains**		**Method of three domains**	
	Steganography images	**Original image**	**Steganography images**	**Original image**
0.45	0.601	0.550	0.796	0.718
0.5	0.528	0.617	0.787	0.743
0.55	0.435	0.713	0.779	0.755
0.6	0.128	0.944	0.772	0.772

Compared with the test of Lie [11] which used two domains (spatial domain and DCT domain), the method of three domains has a higher accuracy in detecting the JPEG images. While the threshold value is 0.55, the accuracy of judging original images is 0.755 (higher than 0.617), and the accuracy of judging steganography images is 0.787 (higher than 0.617). After that, the accuracy by two domains method in classifying steganography images is low while three domains method is not.

4 Conclusions

In this paper, we analyse the F5 steganographic algorithm and the three domains characteristics steganalysis algorithm in JPEG images. Using F5 steganographic system to embed 35.5 kb information into a JPEG image which is 99.7kb, we got the experiment result that when we choose the right k-value, JPEG images could embed information without changing a lot AC coefficients. In other words, F5 algorithm has a high efficiency of embedding information. Three domains steganalysis method is to extract the spatial domain, DCT domain, DWT domain characteristics of the JPEG images. We extract them to train the BP neural network classifier, and classify the images from steganography images and original images by setting the threshold value. The test result indicates three domains steganalysis method could get a higher accuracy than other methods.

References

1. Huayong Ge, Mingsheng Huang. Steganography and Steganalysis Based on Digital Image. 2011 4th International Congress on Image and Signal Processing, pages: 252-255, 2011
2. Xianhua Song, Shen Wang. An Integer DCT and Affine Transformation Based Image Steganography Method. 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, page: 102-105, 2012
3. D.Upham.Jsteg.[EB/OL].ftp://ftp.funet.fi/pub/crypt/steganography/,2007.04.06
4. Outguess.ver.2[EB/OL].http://www.outguess.org,2007.04.10
5. Westfelfeld A. F5-A steganographic algorithm: High capacity despite better steganalysis [C]. New York, Berlin, Heidellberg: Springer-Verlag, 2001.289-302.
6. Yongzhen Zhang, Fenlin Liu. A Method Based on Feature Matching To Identify Steganography Software. 2012 4th International Congress Image and Signal Processing, pages: 989-994, 2012
7. S Lyu, H.Farid Steganalysis Using Color Wavelet Statistics and One-class Support Vector Machine. SPIE Symposmn on Electronic hanging. San Josc CA,2004.
8. Xiangyang Luo, Fenlin Liu. On the Typical Statistic Features For Image Blind Steganalysis. IEEE Journal on Selected Areas in Communication,Vol.29,NO.7, August 2011
9. Harmsen J, Pearlman W. Steganalysis of additive noise modelable information hiding. In Proceedings of the SPIE, Security and Watermarking of Multimedia Contents V, 5020, 131–142
10. Knuth, Donald E.The Art of Computer Programming Vol. 2: Seminumerical Algorithms. Addison Wesley. 1998:694.ISBN0201896842.
11. Lie W, Lin G. A feature-based classification technique for blind image steganalysis[J]. IEEE Transaction on Data Hiding and Multimedia, 2005.7 (6): 1007-1020