Image Steganalysis Based on Statistical Moments of Wavelet Subband Histograms in DFT Domain

Guorong Xuan, Jianjiong Gao
Computer Science Deptartment
Tongji University
Shanghai, China
grxuan@sta.net.cn

Yun Q. Shi, Dekun Zou
Electrical and Computer Engineering Department
New Jersey Institute of Technology
Newark, New Jersey, USA
shi@njit.edu

Abstract- This paper proposed an image steganalysis scheme based on statistical moments of histogram of multi-level wavelet subbands in frequency domain. Our theoretical analysis has pointed out that the statistical moments in frequency domain of histogram is more sensitive to data embedding than the statistical moments of histogram in spatial domain. We test the performance of our proposed scheme over non-blind spread spectrum (SS) data hiding method, blind SS method, block based SS method, LSB method and QIM data hiding methods. Besides, steganographic tools such as Outguess, JSteg and F5 are tested. The experimental results have showed that the proposed method outperforms the prior arts by Farid and Harmsen.

Keywords— Steganalysis; Steganography; Statistical Moments; Histogram; Wavelet decomposition

Topic area—4.a.

I. INTRODUCTION

Steganography is a branch of data hiding. By hiding the very existence of message into innocuous cover media, covert communication is realized. Generally, steganography finds redundant bits in a cover image and embeds a secret message into it. As a result, the natural appearance of the image may be preserved after data hiding. However, the data hiding has introduced some change on the statistical property of the image, which makes steganalysis possible. Image steganalysis is the art to decide if a seemingly innocuous image contains a secret message, thus deterring covert communication.

In [1], the first four statistical moments of wavelet coefficients and their prediction errors of nine high frequency subbands are used to form a 72-dimensional (72-D) feature vector for steganalysis. However, as shown and analyzed later in this paper, the performance in terms of detection rate is not satisfactory, because the selected features are not very sensitive to data hiding process. The steganalysis method based on the mass center of histogram characteristic function has shown improved effectiveness in steganalysis [2]. The performance is however still not high enough because the rather limited number of features cannot achieve high detection rate. In [3] we proposed to use the statistical moments of the Fourier transform of histogram of wavelet subbands and achieved good results.

In this paper, we will analysis the effectiveness of the statistical moments in frequency domain of histogram and the statistical moments in spatial domain of histogram from both theoretic perspective and experimental point of view. Our method can be applied to both BMP non-compressed images and JPEG lossy compressed images. The results are analyzed.

The rest of this paper is organized as following: Section 2 gives the definition of statistical moments in frequency domain (SMF) and statistical moments in spatial domain (SMS); Section 3 discusses in detail about SMF and SMS; Section 4 provides the procedure of our feature extraction method; Section 5 presents the experimental analysis. Conclusion is made in Section 6.

II. STATISTICAL MOMENTS IN FREQUENCY DOMAIN OF HISTOGRAM FOR STEGANALYSIS

The feature for steganalysis is the key to a successful steganalysis. The data hiding process can be modeled as an additive signal, which is independent to the cover image, is add to the cover media [2]. It is well-known that the addition of two independent random signals results in the convolution of two probability density functions (pdf's). We define the statistical moments in frequency domain of histogram and the statistical moments in spatial domain of histogram in (1) and (4) respectively.

The statistical moments in frequency domain of histogram (SMF) M_n:

$$M_n = \sum_{k=-N/2}^{N/2} |f_k|^n \, p(f_k) \qquad (1)$$

where n is the order of moments, N is the length of the DFT of the histogram. f_k is the k-th frequency in DFT ($k=-N/2,\cdots,-1,0,1,\cdots,N/2$), $p(f_k)$ is the frequency distribution of Histogram defined in (2),

$$p(f_k) = |H(f_k)| \Big/ \left(\sum_{k=-N/2}^{N/2} |H(f_k)| \right) \qquad (2)$$

in which $|H(f_k)|$ is the amplitude of DFT of the histogram $h(x_k)$,

$$H(f)=\int_{-\infty}^{\infty}h(x)e^{-j2\pi fx}dx \qquad (3)$$

$h(x_k)$ is the histogram of image, in other words, the number of pixels assuming the value x_k.

For comparison purposes, we define the statistical moments in spatial domain of histogram m_n (SMS) in (4). It is similar to the 1,2,3,4 – order moments defined in [1].

$$m_n=\sum_{k=1}^{N}|x_k|^n\,p(x_k) \qquad (4)$$

n is the order of moments, N is the length of the histogram, x_k is the pixel value, $p(x_k)$ is the distribution of x_k,

$$p(x_k)=h(x_k)\Big/\left(\sum_{k=1}^{N}h(x_k)\right) \qquad (5)$$

III. Property of Histogram of Images

To simplify the discussing, we assume the distribution of histogram as the mixture of two Gaussian distributions. Actually, the histogram of coefficients of wavelet subbands is generally modeled as Laplace. It can be modeled as the mixture of two Gaussion distributions with large variance difference.

A. Gaussian Distribution

For Gaussian distribution, the n-th order absolute moment is defined as [5,,p212]:

$$\int_{-\infty}^{\infty}|x|^n N(0,\sigma^2)dx=k_n\sigma^n \qquad (6)$$

$$where\quad k_n=\begin{cases}\sqrt{2/\pi}, & \forall n=1\\ \sqrt{2/\pi}(n-1)!!, & \forall n\in odd, n>1\\ (n-1)!!, & \forall n\in even, n>1\end{cases}$$

If histogram x is $N(0,\sigma^2)$, the SMS should be

$$m_n=k_n\sigma_n \qquad (7)$$

Its frequency f is $N(0,1/\sigma^2)$. Therefore, the SMF is

$$M_n=k_n/\sigma_n \qquad (8)$$

B. The Mixture of Two Gaussian Signals

Assuming x_1 is $N(0,\sigma_1^2)$, x_2 is $N(0,\sigma_2^2)$ and the a priori probabilities are $P(\omega_1)$ and $P(\omega_2)$, we have $P(\omega_1)+P(\omega_2)=1$. Assuming $\sigma^2=\sigma_1^2,\sigma_2^2=(\beta\sigma)^2$, m_n and M_n will be:

$$m_n=\left(P(\omega_1)+P(\omega_2)\beta^n\right)k_n\sigma^n \quad (9)$$

$$M_n=\left(P(\omega_1)+\frac{P(\omega_2)}{\beta^n}\right)\frac{k_n}{\sigma^n} \quad (10)$$

Assuming the additional noise introduced by data hiding $m\sim N(0,\sigma_m^2)$, and $\sigma_m^2=(\alpha\sigma)^2$, after data hiding, the histogram x_1 is $N(\mu_1,(1+\alpha^2)\sigma^2)$, x_2 is $N(\mu_2,(\alpha^2+\beta^2)\sigma^2)$. For computation convenience, assume $P(\omega_1)=P(\omega_2)=0.5$. The changes of m_n and M_n before and after data hiding are:

$$\left|\frac{\Delta m_n}{m_n}\right|=\frac{(1+\alpha^2)^{n/2}+(\alpha^2+\beta^2)^{n/2}}{1+\beta^n}-1 \qquad (11)$$

$$\left|\frac{\Delta M_n}{M_n}\right|=1-\frac{\left(\beta^2/(1+\alpha^2)\right)^{n/2}+\left(\beta^2/(\alpha^2+\beta^2)\right)^{n/2}}{1+\beta^n} \qquad (12)$$

C. Ratio of the Change of SMF and SMS

From (11) and (12), the ratio of the change of SMF and SMS is

$$R_n=\left|\Delta M_n/M_n\right|\Big/\left|\Delta m_n/m_n\right|=\frac{1+\beta^n-(\frac{\beta^2}{1+\alpha^2})^{n/2}-(\frac{\beta^2}{\alpha^2+\beta^2})^{n/2}}{(1+\alpha^2)^{n/2}+(\alpha^2+\beta^2)^{n/2}-1-\beta^n} \qquad (13)$$

When β assumes 0.0, 0.1 and 1.0, n is 1, 2 and 3, Fig. 1 shows the R_n value with α, in which α ranges from 0.0 to 1. The y-axis is $\ln(R_n)$. Above the Dividing line, $\ln(R_n)>0$, ie. $R_n>1$. In this case, the SMF will change faster than SMS.

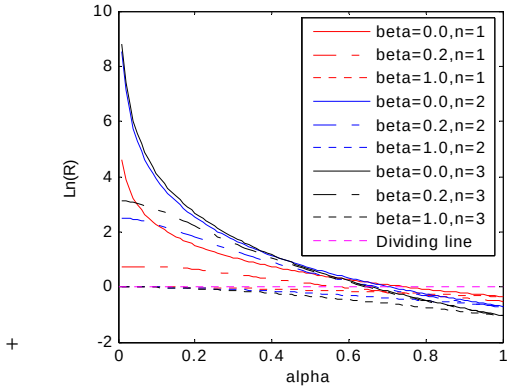

Fig.1 Ratio of the Change of SMF and SMS

We will explain what it means when β is 0, 0.2 or 1.

- If β=0, the histogram is the mixture of a Gaussian signal and a δ function. In wavelet domain, many coefficient will be 0, forming δ function. The rest coefficients form Gaussian distribution.
- If β=1, the two Gaussian signals have the same distribution. The histogram is Gaussian. Generally, this signal cannot represent the natural image.
- If β=0.2, the two Gaussian signals have variances that one is five times of the other. In wavelet domain, a lot small coefficients form a Gaussian with small variance. The rest large coefficients form a Gaussian with large distribution. The mean is zero and the peak is sharp, just like Laplace distribution. Most images fall into this category.

From Fig.1, when α is small, β=0 or 0.2, $\ln(R_n)>0$, the change of SMF is larger than SMS. When α increases, the difference will decrease. Finally, change of SMS will be larger

than SMF. In steganalysis, the variance of the additional noise is small comparing to the image itself. In other words, α will be small. Otherwise, the visual artifact will be seen by human eyes and the purpose of covert communication will be compromised. In wavelet domain, β will be small because of the property of natural image. Then, SMF will be more sensitive than SMS to steganalysis.

D. *Discussion about SMF and SMS*

- Both SMF and SMS can reflect the change of histogram caused by data hiding.
- SMS reflects the change of the histogram with the larger variance. In other word, SMS reflect the overall status of the histogram. For data hiding process, the additional noise will expand the histogram toward both ends. When hidden data is small, the variance of additional noise will be small. As a result, the histogram does not change much overall. Changes on SMS will be small.
- SMF reflects the change of the histogram with the smaller variance. Or, we can say that it reflect the status on the peak of the histogram. For data hiding process, the additional noise will flatten the peak. Even the hidden message is short, the will be obvious change for the peak. Therefore, SMF is sensitive to data hiding.
- Generally, natural images and their wavelet subbands will have peaks. Therefore, SMF will perform better than SMS for natural images.

IV. SMF Based Features

The feature vector for steganalysis consists of multiple SMF of multiple wavelet subbands. The process can be illustrated in Fig.2.

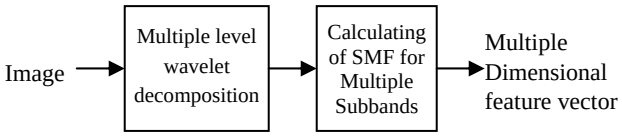

Fig.2 Feature Exaction of the Proposed

We apply a three-level Haar discrete wavelet transformation (DWT) to a test image. Therefore there are 12 subbands, denoted by LL_i, HL_i, LH_i, HH_i, and $i=1,2,3$. The first three moments for each of these 12 subbands and the test image, denoted by LL_0, result in 39 features, or, equivalently a 39-D feature vector.

V. Experimental Results

A. *Experiment 1: SMF and SMS before and after data hiding*

Fig.3 is an image sample from CorelDraw image database [6]. We use JSteg to covert above image in JPG compressed file. Fig.4 is histogram of this JPG file in Spatial domain (left) and frequency domain (right). The blue curve is that of the cover media, the red curve is that of the stego image with 4K data hidden into it using JSteg. Table I is the ratio R_n of the change of SMF and SMS. From Fig.4 and Table I, it is obvious that SMF is more sensitive than SMS. We only give the example for JSteg here due to the length limitation of this paper. Our investigations discover that this observation holds for other data hiding methods also.

Fig. 3 CorelDraw image sample (No. 54010)

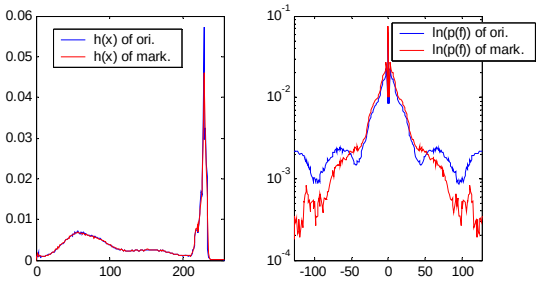

Fig. 4 Histogram in spatial domain (Left), and frequency domain (Right) of image 54010

TABLE I. Ratio of the Change of SMF and SMS

Moment	Cover m_n	Stego m_n	Cover M_n	Stego M_n	R_n
1	68.9	69.0	33.5	22.2	372.9
2	56.4	56.6	24.6	11.4	165.6
3	49.5	49.9	23.0	8.4	100.6

B. *Experiment 2: Experiment on non-compressed images*

The CorelDraw image database contains 1096 images. We first convert the color image s into grey level images. Data are hided into the grey level images. Then the 39-D features are extracted. We randomly select 896 for training and the rest 200 for testing. Bayes classifier is used [4]. Five typical data hiding methods are used to evaluate the proposed steganalysis system: Cox et al's spread spectrum[7]; Piva et al's blind spread spectrum[8], Huang and Shi's block DCT based spread spectrum[9], block DCT based QIM [10] (0.1 bpp) and general LSB [11] data hiding method (0.3 bpp).

The consideration that various data hiding methods, in particular the SS methods, are included in our experimental investigation is justified as follows. Although it may not carry as many information bits as the LSB methods in general, the SS methods can still serve for the covert communication purpose when the payload is not very high. By the way, some newly developed SS methods can hide a large amount of data. For instance, a data embedding rate from 0.5 bpp (bits per pixel) to 0.75 bpp can now be easily achieved [12]. In addition, the SS methods are known more robust than the LSB. Therefore, it is necessary to consider the SS methods for steganalysis.

Table II lists the testing results of the feature of [1], [2] and ours. TN is the detection rate for cover images. TP is the detection rate for stego images. T is the overall detection rate. From Table II, it can be observed that our scheme outperforms previous arts for all data hiding method except 1% lower than that of [1] only for QIM.

TABLE II. STEGANALYSIS RESULTS OF NON-COMPRESSED IMAGE(%)

Date hiding	Farid (72D)			Harmsen (3D)			Ours (39D)		
	TN	***TP***	***T***	***TN***	***TP***	***T***	***TN***	***TP***	***T***
Cox	75	53	64	52	85	68	94	96	95
Piva	86	89	88	91	52	72	89	97	93
Huang	92	61	77	96	64	80	93	98	96
QIM	99	100	99	92	51	71	97	99	98
LSB	90	53	71	81	41	61	93	94	93
combined	86	53	80	98	80	83	87	89	89

C. Experiment 3: Experiment on JPEG compressed images

The same image database is used. The cover color images are generated by applying JSteg[13] or F5 to compress the uncompressed images into JPEG files with quality factor of 75. The stego color images are generated by apply JSteg, F5[14] and OutGuess[15] to the cover images with embedding message size of 1kB(1024Bytes), 2kB and 4kB, the embedding strength is approximately 0.021bpp, 0.041bpp and 0.083bpp accordingly. Feature extraction is achieved by first converting the color images into grey level images, then the 39-D feature are obtained from grey level images. 896 pairs of cover and steg images are trained and the rest 200 are tested and Bayes classifier is used for classifying. It is noted that for OutGuess, some image will fail in hiding certain amount of data. In this case, the test images are still 200 cover and 200 stego, the training images are 896 cover and the rest available stego. The detection rate is reported by averaging over 30 times randomly conducted experiments.

To compare the performance of the proposed method with [1] and [2], we implement their methods and the same Bayes classifier is used. The results are listed in Table III. It can be seen that our method performs better than [1] and [2] for all methods with all embedding strength except in JSteg when embedding strength is 4kB.

TABLE III. JSTEG, F5 AND OUTGUESS STEGANALYSIS RESULTS (%)

Steganography	**Farid (72D)**			**Harmsen (3D)**			**Ours (39D)**		
	TN	***TP***	***T***	***TN***	***TP***	***T***	***TN***	***TP***	***T***
JSteg 1kB	55	70	63	25	83	54	75	69	72
JSteg 2kB	65	83	74	27	85	56	79	75	77
JSteg 4kB	92	92	92	30	87	58	82	83	83
F5 1kB	30	72	51	53	47	50	48	62	55
F5 2kB	51	58	54	44	58	51	53	69	61
F5 4kB	67	60	63	44	60	52	64	77	71
OutGuess1k-	38	52	45	23	75	49	74	73	74
OutGuess1k+	17	64	41	22	75	49	72	73	72
OutGuess2k-	32	78	55	23	80	52	78	76	77
OutGuess2k+	28	78	53	24	79	51	79	77	78
OutGuess4k-	56	89	73	29	82	56	82	82	82
OutGuess4k+	55	86	71	30	81	55	85	82	83

Note: The numbers of successful steg images for OutGuess are: 1095(1kB-), 1071(1kB+), 1063(2kB-), 1001(2kB+), 725(4kB-), 630(4kB+).

VI. CONCLUSION

This paper has discussed the difference between the SMS and SMF, and analyzed their performance in steganalysis from both theoretic and experimental perspective. Experiment results have shown that for both non-compressed images and for JPEG compressed images our SMF based steganalysis scheme outperforms priori arts [1,2] when various data hiding methods are used for covert communication.

ACKNOWLEDGMENT

This research is supported partly by National Natural Science Foundation of China (NSFC) on the project "The Research of Theory and Key Technology of Lossless Data Hiding (90304017)", and by New Jersey Commission of Science and Technology via New Jersey Center of Wireless Networking and Internet Security (NJWINS).

REFERENCES

[1] H.Farid. Detecting hidden messages using higher-order statistical models. In: Proc. of the IEEE Int'l. Conf. on Image Processing 02[C], Vol II. New York: IEEE, 2002. 905~908.

[2] J. J. Harmsen. Steganalysis of Additive Noise Modelable Information Hiding. Rensselaer Polytechnic Institute, Troy, New York , May 2003.

[3] Y. Shi, G. Xuan, C. Yang, J. Gao, Z. Zhang, P. Chai, D. Zou, C. Chen, W. Chen. Effective Steganalysis Based on Statistical Moments of Wavelet Characteristic Function. Intl. Conf. on Infor. Tech., April 4-6, 2005, Las Vegas, USA.

[4] R. O. Duda, P. E. Hart, D. G. Stork. Pattern Classification, Second Edition. John Wiley & Sons, 2001.

[5] Su Chun, Probability Theory, Science Publisher, (in Chinese), China, March 2004.

[6] CorelDraw Software: http://www.corel.com.

[7] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon. Secure Spread Spectrum Watermarking for Multimedia[J]. IEEE Trans. on Image Processing, 1997，6(12):673-1687.

[8] A.Piva, M.Barni, E.Bartolini, V.Cappellini: DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image. In: Proc. of the 1997 Intl. Conf. on Image Processing vol.1, P.520.

[9] J. Huang and Y. Q. Shi: An Adaptive Image Watermarking Scheme Based on Visual Mask-ing. In: IEE Electronic Letters, 1998, 34(8):748-750.

[10] B. Chen and G. W. Wornell: Digital watermarking and information embedding using dither modulation. In: Proceedings of IEEE MMSP 1998, pp273 – 278.

[11] K. Matsui and K. Tanaka: Video-steganography: How to secretly embed a signature in a picture." Journal of the Interactive Multimedia Association Intellectual Property Project, vol.1, pp. 187-205, Jan. 1994.

[12] G. Xuan, Y. Q. Shi, Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," Proceeedings of International Workshop on Diigtal Watermakring, Seoul, Korea, October 2004.

[13] Steganography software for Windows: http://members.tripod.com/stego/software.html.

[14] Westfeld, A. High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm). In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, Vol.2137. Springer-Verlag, 2001, pp. 289–302

[15] Provos, N. and Honeyman, P. Detecting Steganographic Content on the Internet. CITI Technical Report 01-11, 2001