ESTIMATION OF MB STEGANOGRAPHY BASED ON LEAST SQUARE METHOD

Mankun Xu, Tianyun Li, Xijian Ping

National Digital Switching System Engineering & Technological Research Center

ABSTRACT

In the available Jpeg steganography methods, Model-based (MB) steganography technique is more secure than Jsteg, F5 and OutGuess. In this paper, we consider the problem of estimating the embedded length of secret messages of MB steganography. We provide an expected distribution of the non-zero AC coefficients' high precision histogram to fit the stegotexts', and adopt the cropped and recompressed calibration to obtain the carrier image approximation. Then, we present a new algorithm to estimate the embedding rates based on least square method. The attacks towards MB are successful with experimental evidence on 2700 carrier images and the stego images of different quality factor and different embedding rates.

Index Terms— steganography, steganalysis, generalized Cauchy distribution, least square method

1. INTRODUCTION

Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuour-looking cover media objects, such as images, using the human's visual, aural redundance or media objects' statistical redundance. Conversely, the purpose of steganalysis is to expose the existance of secret message. It aims to detect, extract or destroy the secret message by finding "difference" between cover and stego images. In the available image formats, Jpeg is the most popular types as image carriers for steganography.

Jsteg [1] seems to be the first steganographic tool to embed into JPEG images. It adopts the similar embedding scheme to the spatial LSB replacing, and is accomplished by replacing the LSB of quantised non-zero DCT coefficients. This method has defects of pair wise of adjacent bins in the DCT histogram and can be easily attacked by Chi-square analysis. To improve the embedding security, the F-series algorithms, especially F5 [2] adapts the LSB to the message by decreasing the coefficients' absolute values. In addition, F5 implements Matrix encoding and a permutative straddling function to resist the attacks. Although F5 has a significant security improvement over Jsteg, it has leaks in the histogram which is more sharpen and shrinkable than the origin's. C. Hong *et al* [3] present an accurate estimate for the length of the embedded secret message of F5. OutGuess [4] is another classical steganographic tool which can hold the first order statistics by preserving about half length of the maximum coefficients in order to realize plausible deniability. OutGuess also has the blockiness increasing like other Jpeg embedding methods. J. Fridrich *et al* [5] give out an length estimation of embedded message of OutGuess. Unlike the above Jpeg steganographic tools, MB methods present a new novel framework in a different angle of view. MB [6] Jpeg steganography devises the carrier X into a deterministic and in-deterministic random variables as $X = (X_{\text{det}}, X_{\text{indet}})$. The low precision histograms of non-zero DCT AC coefficients aren't changed, while the high precision histograms are changed according to the probabilities fitting the generalized Cauchy distribution. MB methods are more secure than the previously Jpeg steganography methods. Until now, the targeted attacks to MB is few, especially in estimating the length of the embedding messages. Böhme *et al* [7] present a detection method with first order statistics to break MB. And, quite a few universal blind detectors have been proposed to detect virtually every steganographic method after training on a database of stego and cover images [8-10]. They have obtained good effects but do not allow accurate estimation of the embedded messages.

2. MB STEGANOGRAPHY FOR JPEG IMAGES

MB steganography modifies the LSB of the coefficients to hide secret message. Let us define $h^{i,j}$ as the high precision histogram of non-zero AC coefficients (with bin size > 1) in location (i, j) $(i, j = 1,2,\ldots 8, i, j$ are not equal to 1 simultaneously). Let $h_k^{i,j}$ denote the number of $\text{DCT}^{(i,j)}$ coefficients equal to k-th high precision bin of $h^{i,j}$. $l_k^{i,j}$ denotes the low precision bin comprising several high precision bins。Let the bin size equal to 2, the low and high precision bins can be represented as:

$$l_k^{i,j} = \begin{cases} h_{2k+1}^{i,j} + h_{2k}^{i,j} & k < 0 \\ h_0^{i,j} & k = 0 \\ h_{2k-1}^{i,j} + h_{2k}^{i,j} & k > 0 \end{cases} \quad (1)$$

The MB embedding process is:

(1). Generate the low precision (bin size > 1) histograms of coefficient values for all 63 AC blocks. Model each histogram with the generalized Cauchy distribution and fit the parameters of β and s by maximum likelihood.

$$f(u \mid \beta, s) = \frac{\beta - 1}{2s}(|u / s| + 1)^{-\beta} \tag{2}$$

where u is the coefficient value, $\pi > 1$, $s > 0$.

(2). Compute the probability of each possible coefficient value for each coefficient using the model cumulative density function.

For $k > 0$, from Eq. (1) there exists:

$$p\left(h_{2k-1}^{i,j} \middle| l_k\right) + p\left(h_{2k}^{i,j} \middle| l_k\right) = 1 \tag{3}$$

$$\text{Where, } p\left(h_{2k-1}^{i,j} \middle| l_k\right) = \frac{f\left(2k-1 \middle| \beta, s\right)}{f\left(2k-1 \middle| \beta, s\right) + f\left(2k \middle| \beta, s\right)} \tag{4}$$

(3). Generate a pseudo-random permutation to determine the ordering of the coefficients.

(4). Pass the message, and the symbol probabilities computed in step 2 in the order specified by step 3 to a non-adaptive arithmetic decoder to obtain symbols specifying the new bin offsets for each coefficient.

3. MB STEGANALYSIS

3.1. AC coefficient histogram

Denote the embedding rate as α, $0<\alpha<1$, there are α*100% non-zero AC coefficients embedded and the left $(1-\alpha)$*100% aren't changed. Denote $\hat{h}^{i,j}$ and $\widehat{hh}^{i,j}$ as the total coefficient and the embedded coefficient high precision histogram of stego images, $\overline{h}^{i,j}$ and $\overline{hh}^{i,j}$ as the expected histogram of $\hat{h}^{i,j}$ and $\widehat{hh}^{i,j}$. Böhme *et al* [7] model the symbol output of the arithmetic decoder as a Bernoulli distributed random variable at the maximum-length embedding rate. Here, we model:

$$\begin{cases} \widehat{hh}_{2k-1}^{i,j} \sim B\left(l_k^{i,j},\ p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right)\right) \\ \widehat{hh}_{2k}^{i,j} \sim B\left(l_k^{i,j},\ 1\text{-}p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right)\right) \\ \widehat{hh}_{-2k+1}^{i,j} \sim B\left(l_{-k}^{i,j},\ p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right)\right) \\ \widehat{hh}_{-2k}^{i,j} \sim B\left(l_{-k}^{i,j},\ 1\text{-}p\left(h_{-2k}^{i,j} \middle| l_{-k}^{i,j}\right)\right) \end{cases} k > 0 \tag{5}$$

The expected high precision bin $\overline{hh}^{i,j}$ is given by the expected values of Bernoulli distribution:

$$\begin{cases} \overline{hh}_{2k-1}^{i,j} = E\left[B\left(l_k^{i,j},\ p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right)\right)\right] = l_k^{i,j} * p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right) \\ \overline{hh}_{2k}^{i,j} = l_k^{i,j} * \left(1 - p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right)\right) \\ \overline{hh}_{-2k+1}^{i,j} = E\left[B\left(l_{-k}^{i,j},\ p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right)\right)\right] = l_{-k}^{i,j} * p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right) \\ \overline{hh}_{-2k}^{i,j} = l_{-k}^{i,j} * \left(1 - p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right)\right) \end{cases} k > 0 \tag{6}$$

The expected high precision bin $\overline{h}^{i,j}$ in location (i, j) can be represented as the following four equations:

$$\overline{h}_{2k-1}^{i,j} = \alpha l_k^{i,j} p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right) + (1-\alpha) h_{2k-1}^{i,j} \tag{7}$$

$$\overline{h}_{2k}^{i,j} = \alpha l_k^{i,j} \left(1 - p\left(h_{2k}^{i,j} \middle| l_k^{i,j}\right)\right) + (1-\alpha) h_{2k}^{i,j} \tag{8}$$

$$\overline{h}_{-2k+1}^{i,j} = \alpha l_{-k}^{i,j} p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right) + (1-\alpha) h_{-2k+1}^{i,j} \tag{9}$$

$$\overline{h}_{-2k}^{i,j} = \alpha l_{-k}^{i,j} \left(1 - p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right)\right) + (1-\alpha) h_{-2k}^{i,j} \tag{10}$$

3.2. Estimation of embedding rates

For the steganalysis, the carrier's $h^{i,j}$ is unkown, so we first calibrate the detected image by using the calibration method proposed by Fridrich *et al*[8]. Denote the calibrated high and low precision histograms as $\tilde{h}^{i,j}$ and $\tilde{l}^{i,j}$. To reduce the effects of probably imprecise calibration, we adopt the method of least square method to decrease the dependence on calibration.

For k > 0, from Eq. (7)-(10), there exists:

$$\sum_{k>0}\left(h_{2k-1}^{i,j} - \tilde{h}_{2k-1}^{i,j}\right)(1-\alpha) \approx \sum_{k>0}\left[\left(\tilde{h}_{2k-1}^{i,j} - l_k p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right)\right)\alpha + \left(\overline{h}_{2k-1}^{i,j} - \tilde{h}_{2k-1}^{i,j}\right)\right] \tag{11}$$

Define $a = \sum_{k>0}\left(\tilde{h}_{2k-1}^{i,j} - l_k p\left(h_{2k-1}^{i,j} \middle| l_k^{i,j}\right)\right)$, $b = \sum_{k>0}\left(\hat{h}_{2k-1}^{i,j} - \tilde{h}_{2k-1}^{i,j}\right)$ and replace $\overline{h}^{i,j}$ by $\hat{h}^{i,j}$, there is:

$$\sum_{k>0}\left(h_{2k-1}^{i,j} - \tilde{h}_{2k-1}^{i,j}\right)(1-\alpha) = a\alpha + b \tag{12}$$

In the same manner,

$$\sum_{k>0}\left(h_{2k}^{i,j} - \tilde{h}_{2k}^{i,j}\right)(1-\alpha) = c\alpha + d \tag{13}$$

$$\sum_{k>0}\left(h_{-2k+1}^{i,j} - \tilde{h}_{-2k+1}^{i,j}\right)(1-\alpha) = e\alpha + f \tag{14}$$

$$\sum_{k>0}\left(h_{-2k}^{i,j} - \tilde{h}_{-2k}^{i,j}\right)(1-\alpha) = g\alpha + h \tag{15}$$

Where, $c = \sum_{k>0}\left(\tilde{h}_{2k}^{i,j} - l_k p\left(h_{2k}^{i,j} \middle| l_k^{i,j}\right)\right)$, $d = \sum_{k>0}\left(\hat{h}_{2k}^{i,j} - \tilde{h}_{2k}^{i,j}\right)$,

$e = \sum_{k>0}\left(\tilde{h}_{-2k+1}^{i,j} - l_{-k} p\left(h_{-2k+1}^{i,j} \middle| l_{-k}^{i,j}\right)\right)$, $f = \sum_{k>0}\left(\hat{h}_{-2k+1}^{i,j} - \tilde{h}_{-2k+1}^{i,j}\right)$,

$g = \sum_{k>0}\left(\tilde{h}_{-2k}^{i,j} - l_{-k} p\left(h_{-2k}^{i,j} \middle| l_{-k}^{i,j}\right)\right)$, $h = \sum_{k>0}\left(\hat{h}_{-2k}^{i,j} - \tilde{h}_{-2k}^{i,j}\right)$.

For example of Eq. (12), the estimation is carried based on least square method:

$$\Delta_1 = \min\left[\sum_{k>0}\left(h_{2k-1}^{i,j} - \tilde{h}_{2k-1}^{i,j}\right)(1-\alpha)\right]^2 = a^2\alpha^2 + 2ab\alpha + b^2$$

$$\frac{\partial \Delta_1}{\partial \alpha} = 2a^2\alpha + 2ab \tag{16}$$

$$\frac{\partial \Delta_2}{\partial \alpha} = \frac{\partial \min\left[\sum_{k>0}\left(h_{2k}^{i,j} - \tilde{h}_{2k}^{i,j}\right)(1-\alpha)\right]^2}{\partial \alpha} = 2c^2\alpha + 2cd \tag{17}$$

$$\frac{\partial \Delta_3}{\partial \alpha} = \frac{\partial \min\left[\sum_{k>0}\left(h_{-2k+1}^{i,j} - \tilde{h}_{-2k+1}^{i,j}\right)(1-\alpha)\right]^2}{\partial \alpha} = 2e^2\alpha + 2ef \tag{18}$$

$$\frac{\partial \Delta_4}{\partial \alpha} = \frac{\partial \min\left[\sum_{k>0}\left(h^{i,j}_{-2k} - \tilde{h}^{i,j}_{-2k}\right)(1-\alpha)\right]^2}{\partial \alpha} = 2g^2\alpha + 2gh \quad (19)$$

Let Eq. (16)-(19) equal to 0, we will get the estimation values. The results of a large number of Jpeg images show that the average values of solutions of Eq. (16)-(19) can obtain the best estimation. The average results are shown in chapter 4.

We know that the most of AC coefficients are zero or near zero, especially in the high frequency location after Zigzag scanning. And the calibration can not obtain exactly original carriers. So in applications, we can only choose the locations where the calibrated histograms fit the carrier well. And, the value k is set small integers. In this way, the computational complexity is decreased greatly and the estimation precision is ensured.

Outline of our method towards MB:

(1). Generate 63 low precision histograms $l^{i,j}_k$ of AC values, fit the parameters β and s of the parametric generalized Cauchy distribution model, compute $p\left(h^{i,j}_{2k-1}|l_k\right)$ and $p\left(h^{i,j}_{2k}|l_k\right)$ for each high precision bin by Eq. (2) - (4).

(2). Calibrate the detected image to approximate the carrier, and compute the high precision histograms $\tilde{h}^{i,j}_k$.

(3). Estimate the embedding rates by solution of Eq. (16)-(19). When $\alpha<0$, let $\alpha=0$ and when $\alpha>1$, let $\alpha=1$.

4. EXPERIMENTAL RESULTS AND ANALYSIS

We use 2700 NRCS images which can be downloaded from http://photogallery.nrcs.usda.gov, each resized to 716 * 512 by converted to grayscale images and then compressed to Jpeg image with q.f. 75. The test image database are embedded by MB at $\alpha = 0.2, 0.4, 0.6, 0.8, 1$. Here we only choose $k \in [1, 2, .., 5]$ and limit the computations in the range $\left|\tilde{l}^{i,j}_k - l^{i,j}_k\right| \Big/ l^{i,j}_k \le 0.1$. The figures from 1 to 6 plot the estimation results, where the horizontal coordinate represents the image numbers, and the vertical one represents the estimation. Table 1 lays out the estimation mean and standard deviation results.

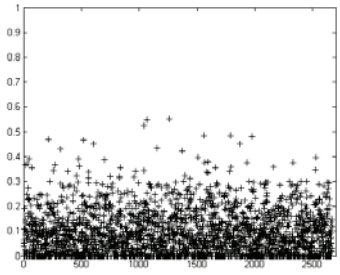

Fig. 1: estimation of carriers

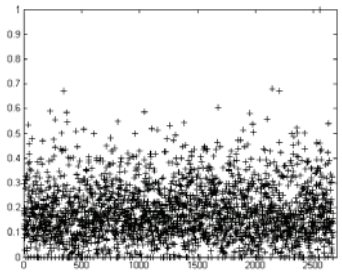

Fig. 2: estimation of stego images at $\alpha = 0.2$

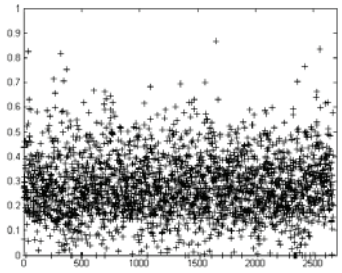

Fig. 3: estimation of stego images at $\alpha = 0.4$

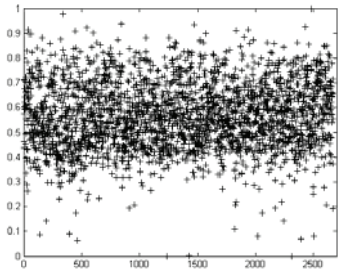

Fig. 4: estimation of stego images at $\alpha = 0.6$

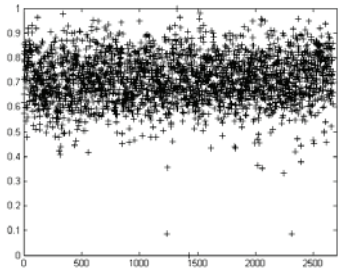

Fig. 5: estimation of stego images at $\alpha = 0.8$

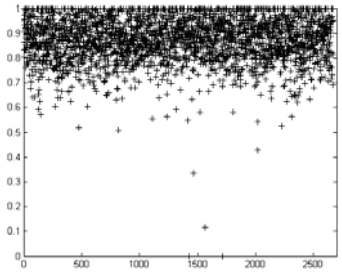

Fig. 6: estimation of stego images at $\alpha = 1$

Table 1: the mean and standard deviation of results

estimation	embedding rates					
	0	0.2	0.4	0.6	0.8	1
mean	0.0870	0.1725	0.3274	0.5647	0.7120	0.8749
std	0.1148	0.1213	0.1041	0.1232	0.1368	0.1265

Fig. 7 gives the ROC curves of our method to detect MB. For comparison, Fig. 8 gives the ROC curves of the method in [7]. The ROC curves represents $\alpha = 1, 0.6, 0.6, 0.4, 0.2$ from top line to the bottom line denoted by "□, *, +, ○, ◇".

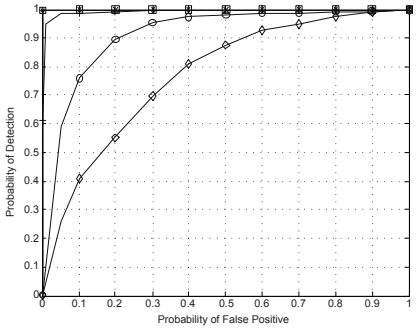

Fig. 7: ROC curves of our method

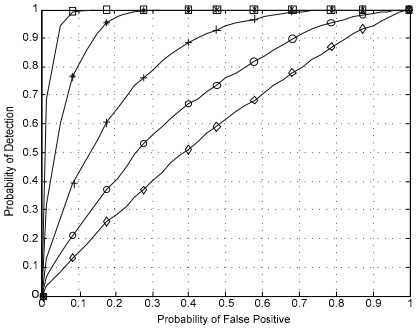

Fig. 8: ROC curves of the method in [7]

The above figures and table indicate that our method has good ability to estimate the embedding rates. Observe the ROC curves in Fig. 7 and Fig. 8, our method outperforms the method presented by Böhme [7]. The detection performance of our method is very good especially when $\alpha > 0.4$. In table 1, we can see that the standard deviations of the results are not very small. This is because in the process of MB steganography, the fitting of the model parameters β and s using MLE are not very precise, especially in the condition of few AC coefficients. And, the calibration of the detected image inevitably differs from the cover images. Another reason that cannot be neglected is that the arithmetic decoding couldn't decode the random secret message by the exact probability of high precision bins. So, if the more reasonable parametric model of AC coefficient histograms could be studied, the better assumptions of expected high precision bin $\overline{h}^{i,j}$ can be obtained, and the estimation will be more precise.

5. CONCLUSIONS AND FUTURE WORK

In this paper, we present a novel method to estimate the embedding rates towards MB JPEG steganography. We give out the expected distribution of high precision bins of non-zero AC coefficients, and solute those functions to estimate the embedding rate based on least square method. The experimental results of 2700 Jpeg images show the good performance of our method. In the future, we will develop further study on the better model of AC coefficient histograms to improve it.

6. FOOTNOTES REFERENCES

[1] Avcibas, M. Kharrazi, N.D. Memon, and B. Sankur, "Image steganalysis with binary similarity measures," EURASIP Journal on Applied Signal Processing, No. 17, pp. 2749-2757, 2005.

[2] A. Wstfeld, "F5-a steganographic algorithm high capacity despite better steganalysis," Lecture notes in computer science, No. 2137, Vol.2, pp. 289-302, 2001.

[3] C. Hong, S.S. Agaian, and Y. Wang, "An Effective Algorithm for Breaking F5," In IEEE 7th Workshop, Multimedia Signal Processing, Shanghai, China, pp. 1-4, 2005.

[4] N. Provos, "OutGuess – Universal Steganography," 2001, http://www.outguess.org/.

[5] J. Fridrich, M. Goljan, and D. Hogea, "Attacking the outguess," In ACM Special Session on Multimedia Security and Watermarking, Juan-les-Pins, France, pp. 2002.

[6] P. Sallee, "Model-Based Steganography," International Workshop on Digital Watermarking, 2939, pp. 154-167, 2004.

[7] R. Böhme, and A. Westfeld, "Breaking Cauchy Model-Based JPEG Steganography with First Order Statistics," In proceedings of ESORICS , Springer-Verlag, pp. 125-140, 2004.

[8] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," Proc. of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, San Jose, CA, 6072, pp. 1-13, 2006.

[9] T. Pevný, and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis," Proc. of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, 6505, pp. 3-4, 2007.

[10] Y.Q. Shi, C. Chen, and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," In the 8th International Workshop of Information Hiding, 4437 of Lecture Notes in Computer Science, New York, pp. 249-264, 2006.