Extended Optimization Method of LSB Steganalysis

Xiaoyi Yu, Tieniu Tan, Yunhong Wang
National Laboratory of Pattern Recognition, Institute of Automation,
Chinese Academy of Sciences, P.O. Box 2728, Beijing, 100080, P.R. China
E-mails: {xyyu,wangyh,tnt }@nlpr.ia.ac.cn

***Abstract*—Image steganalysis has attracted increasing attention recently. LSB steganalysis is one of the most active research topics. The paper proposes a method for LSB steganalysis of images, where the secret message is embedded in a given number L of the least significant bits. The proposed estimation method is an extension of Fridrich's method from the case L = 1 to arbitrary L>0. A weighted stego image is defined first and then estimation formula is derived. To evaluate the proposed steganalytic method, two experiments of detection and estimation are performed. It is shown that the accuracy of detecting the existence of secret messages in images and of estimating the embedding ratio of secret messages is relatively high. Estimation errors and further studies are also discussed. Experimental results and theoretical verification show that this mehtod is an effective method of LSB steganalysis.**

Keywords-Steganography; LSB; Steganalysis; Eestimation

I. INTRODUCTION

Steganography aims to hide the very presence of communication. That is to say, the essential goal of steganography is to conceal the facts of a hidden message. Similar to cryptanalysis, steganalysis attempts to defeat the goal of steganography. The most popular and frequently used steganographic method is the Least Significant Bit embedding (LSB). LSB stegangraphy is based on manipulating the LSB planes by directly replacing the LSBs of the cover-image with the message bits. In the literature, many techniques about data hiding are based on LSB [1,2], and the vast majority of steganographic programs[3] available for download on the Internet use LSB embedding (Steganos II, S-Tools 4.0, Steghide 0.3, and many others). For the convenience of description, we denote the binary representation of the pixel value of an image as "$b_q b_{q-1} \cdots b_L \cdots b_1$," where q is the number of bits to represent image pixel value, b_q , b_L and b_1 are the Most Significant bit (MSB) , Lth-rightmost bit and Least significant bit (LSB) respectively. Some LSB methods modify L rightmost significant bits, such as simple LSB substitution [1] and Bit-Plane Complexity Segmentation Steganography (BPCS) [2], while almost all the steganographic programs only modify b_1 . The popularity of the LSB embedding shows that the reliable detection of LSB steganography is an important research topic.

There are numerous methods for the detection of LSB steganography [4-9]. Almost all the proposed steganalytic techniques except [9,10] are designed to attack the LSB steganography for the case L=1and cannot be extended to L>1. Niimi [10] studies the complexity histogram of an image and points out an anomaly in its shape. It is a visual-attack like technique, and hard to detect the existence of steganography automatically. The reliability of this technique is questionable. The technique is only for BPCS method, and hard to be extended to attack L>1. In [9], we proposed a method based on isotropy analysis, which is currently the first steganalysis method to attack LSB steganography for the case L>1. The method can not only detect the existence of hidden message, but also estimate the hidden message length.

In this paper, a new method on estimating hidden message length of the case L>1 is proposed. The method is enlightened by the estimation method of [6]. So the advantage of this method is also its clean and quite simple mathematical derivation. In the next section, we explain the estimation method of [6]. In Section 3, we explain an assumption of natural images. Based on the assumption, the details of the detection and estimation scheme are presented in Section 4, and the experimental results are given in Section 5. Some related issues and problems for future study are discussed in Section 6.

II. FRIDRICH'S SCHEME

The goal of this section is to explain Fridrich's estimation scheme [6].

Let $X = \{x_i\}_{i=1}^{n}$ be a column vector of integers in the range [0, 255] representing a grayscale cover image with n=Mx×Nx pixels. Let *S={si}* denote the stego image after embedding qn bits, 0 ≤ q ≤ 1, using LSB embedding (L=1) in qn pixels randomly selected from the cover image *X*. Let $S^p = \{s_i^{(p)}\}$ be the "weighted" stego image, $s_i^{(p)} = s_i + (\overline{s}_i - s_i)\dfrac{p}{2}$, $0 \le p \le 1$, $\overline{s}_i = s_i + 1 - 2(s_i \% 2)$, $i = 1, \cdots, n$. Then S^q is the closest weighted stego image to X in least square sense. This gives the idea to estimate the secret message length as an optimization problem. The estimation formula is derived as:

$$\overline{q} = -(2/n)\sum\nolimits_{i=1}^{n}(s_i - F(N(s_i)))(\overline{s}_i - s_i) \qquad (1)$$

The work is sponsored by the Natural Science Foundation of China (under grants No. 60172054, No. 60121302 and No. 60335010) and the National 973 program (Grant No. 2004CB318100).

where $F(N(s_i))$ is the estimated pixel value of cover image from the neighborhood. The formula is clean and simple. The experimental results show good estimation performance of Equation (1). The authors of [6] also have analyzed the estimation error and proposed the improvements.

III. SYMMETRY OF IMAGE PIXELS

Assumption: Let $L \in \{1, 2, \cdots, q\}$, $l \in \{1, \cdots, 2^L - 1\}$, $k \in \{0, 1, \cdots, 2^{q-L} - 1\}$, and $h(l)$ denotes the total number of pixels in images whose pixel value is $x_i = 2^L k + l$. For natural images, we have:

$$h(0) = h(1) = \cdots h(2^L - 1) = n/2^L \tag{2}$$

The assumption means that image pixels have a kind of symmetric property. For example, if L=1, this is the case that the numbers of pixels in an image with odd and even intensity values are roughly the same.

TABLE 1
TEST RESULTS OF ASSUMPTION

L	1	2	3	4
ratio	0.9950	0.9500	0.9350	0.9100

So $h(l)$ follow a uniform distribution. The property of whether the distribution $h(l)$, $l \in \{1, \cdots, 2^L - 1\}$ are Uniform or not is taken using hypothesis testing. The Null and the Alternative hypotheses in this case are:

$$\text{H0: } h(l) = n/2^L \tag{3.a}$$

$$\text{H1: } h(l) \neq n/2^L \tag{3.b}$$

where $l \in \{1, \cdots, 2^L - 1\}$.

In order to evaluate the validity of this assumption, statistical tests are carried out using the Chi-square test. The χ^2 statistic is given as:

$$\chi^2 = \sum_{n=0}^{2^L-1} \frac{(h(l) - n/2^L)^2}{(h(l) + n/2^L)/2} \tag{4}$$

Let χ_α^2 denotes the upper tabulated value of Chi-square distribution at significant level α and $2^L - 1$ degree of freedom. For an image that obeys the assumption, we have:

$$\chi^2 < \chi_\alpha^2 \tag{5}$$

The statistical tests are carried out on the Corel Image Database (only 5200 JPEG images in CD1 were used) [11]. In our experiments, we take the case of L=1,2,3,4 (Table 1) as examples to test the assumption. The significant level for chi-square test in Equation (5) is set to 0.05. The experimental results are shown in Table 1. In the table, the ratios of the number of images that obey Equation (2) to the total number of images (5200) are listed. From the tables we can see that the assumption is appropriate for most natural images.

IV. EXTENDING THE OPTIMIZATION METHOD

Inspired by the estimation method of [6], we extend Fridirich's method [6] from the case L = 1 to arbitrary L>0. We first extend the optimization theorem of [6]. The definition of X is the same as [6].

Theorem 1: Let S={s_i} be the image after embedding qnL bits, 0 ≤ q ≤ 1, using LSB embedding (L>0) in qn pixels randomly selected from the cover image X. Let $S^p = \{s_i^{(p)}\}$ be the "weighted" stego image, $s_i^{(p)} = s_i + (2^L - 1 - 2(s_i \% 2^L))\, p/2$, $0 \le p \le 1$, $i = 1, \cdots, n$, then:

$$q = \arg\min_p E(p)$$
$$E(p) = \frac{1}{n}\sum_{i=1}^{n} (s_i^{(p)} - x_i)^2 \tag{6}$$

Proof:

$$E(p) = \frac{1}{n}\sum_{i=1}^{n} (s_i^{(p)} - x_i)^2$$
$$= \frac{1}{n}\sum_{i=1}^{n} (s_i - x_i + (2^L - 1 - 2(s_i \% 2^L))\, p/2)^2$$

Let $A = \frac{1}{n}\sum_{s_i = x_i} (s_i - x_i + (2^L - 1 - 2(s_i \% 2^L))\, p/2)^2$,

$B = \frac{1}{n}\sum_{s_i \neq x_i} (s_i - x_i + (2^L - 1 - 2(s_i \% 2^L))\, p/2)^2$.

In the case of data hiding in the L-rightmost bits of a pixel, the pixel value has equal possibility to become any one of the remaining $2^L - 1$ pixel values with the probability of $p/2^L$, and a pixel keeps unchanged with the probability of $1 - (2^L - 1)\, p/2^L$. So combining the assumption described in the last section, we have:

$$A = (1/n)\{(1 - q(2^L - 1)/2^L)\, n/2^L [$$
$$(p(2^L - 1)/2)^2 + (p(2^L - 3)/2)^2 + \cdots p^2/4 +$$
$$(-p/2)^2 + (-3p/2)^2 + \cdots (-p(2^L - 1)/2)^2]\}$$

$$B = \frac{1}{n}\{\frac{q}{2^L}\frac{n}{2^L}[(p(2^L - 1)/2 - 1)^2 +$$
$$(p(2^L - 1)/2 - 2)^2 + \cdots$$
$$+(p(2^L - 1)/2 - 2^L + 1)^2 +$$
$$(p(2^L - 1)/2 + 1)^2 + (p(2^L - 3)/2 - 1)^2 + \cdots$$
$$+(p(2^L - 3)/2 - 2^L + 2)^2 + \cdots$$
$$(p/2 + 2^{L-1} - 1)^2 + (p/2 + 2^{L-1} - 2)^2 + \cdots$$
$$+(p/2 - 2^{L-1})^2 +$$

$$(-p/2+2^{L-1})^2+(-p/2+2^{L-1}-2)^2+\cdots$$
$$+(-p/2-2^{L-1}+1)^2+\cdots$$
$$+(-p(2^L-1)/2+2^L-1)^2$$
$$+(-p(2^L-1)/2+2^L-2)^2$$
$$+\cdots(-p(2^L-1)/2+1)^2]\}$$

let $\sigma=\sum_{k=1}^{2^{L-1}}(2k-1)$, we obtain:

$$dE(p)/dp=d(A+B)/dp$$
$$=[(1-q)p+(p-1)q]\sigma/2^L$$

which proves the fact that $E(p)$ reaches its minimum at $p=q$.

Using Equation (2), we can estimate the secret message length. However, x_i is unknown for estimation. We use the same estimator as [6], which is shown as follows:

$$\overline{x}_{kj}=(x_{k+1j}+x_{k-1j}+x_{kj+1}+x_{kj-1})/4 \qquad (7)$$

However, Theorem 1 cannot be used to estimate the secret message length directly. We derive another concise formula for estimation as follows:

Theorem 2: Let S={s_i} be the image after embedding qnL bits, 0 ⩽ q ⩽ 1, using LSB embedding (L>0) in qn pixels randomly selected from the cover image X. Let $\overline{x}_i$ be the estimator as [7], then:

$$\overline{q}=\arg\min_p E_1(p)=\frac{2}{n}\sum_{i=1}^{n}\frac{s_i-\overline{x}_i}{2^L-1-2(s_i\%2^L)} \qquad (8)$$

where $\overline{q}$ is an estimate of hidden message length and

$$E_1(p)=\frac{1}{n}\sum_{i=1}^{n}(s_i^{(p)}-\overline{x}_i)^2 \qquad (9)$$

Proof:

$$E_1(p)=\frac{1}{n}\sum_{i=1}^{n}(s_i^{(p)}-\overline{x}_i)^2$$
$$=\frac{1}{n}\sum_{i=1}^{n}(s_i-\overline{x}_i+(2^L-1-2(s_i\%2^L))\,p/2)^2$$

according to **Theorem 1**, the minimum of E$_1$(p) is reached for p that satisfies the following equation:

$$\frac{dE_1(p)}{dp}=\frac{1}{n}\sum_{i=1}^{n}\frac{d(s_i-\overline{x}_i-2^L+1+2(s_i\%2^L))}{dp}=0$$

which gives (8).

V. EXPERIMENTAL RESULTS

In order to evaluate the extended estimation method, four experiments are performed here. Our experiments are carried out to test LSB steganography with randomly scattered message bits. In our experiments, we take the case of L=1,2,3 and 4 as examples to test the effectiveness of our proposed steganalysis framework.

We first consider the case of L=1. We have generated 4 stego images for each image in Corel Image Database (10000 JPEG images totally) [11] and the length of hidden messages are 20, 40, 60 and 80 percentage of hiding capacity, corresponding to p=0.2, 0.4,0.6, 0.8, with the case of L=1.

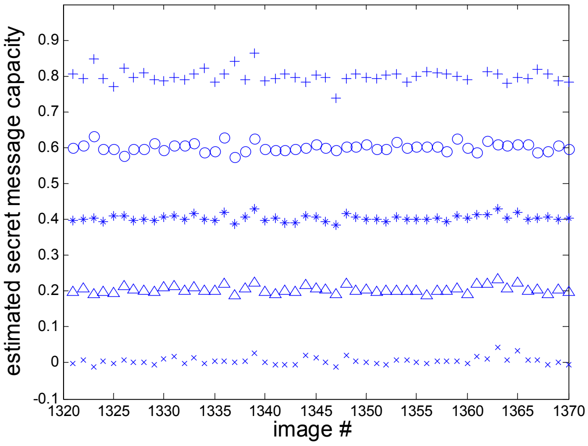

Fig. 1 Estimated embedding ratio of part images from image database at L=2

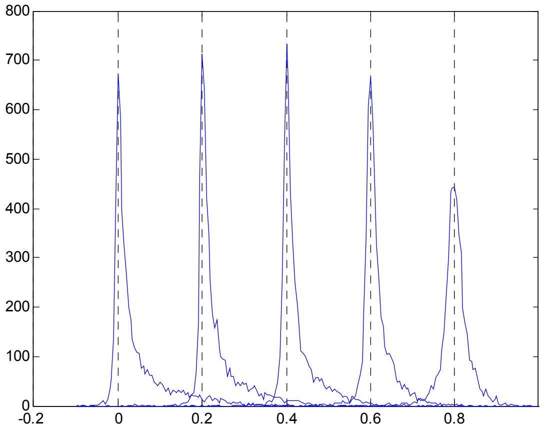

Fig. 2. Distribution of estimated embedding ratio (dashed lines are true ratios) at L=2

The embedding process is just as the process described in Section 3.1, and the secret message is embedded into the L-rightmost LSBs of the cover-image. $p=n'/(M_C\times N_C)$. After the embedding process, we estimate the embedding ratio using Equation (8). For the case of L=2,3 and 4, the tests are carried out as the case of L=1.

For the convenience of display, only parts of experimental results are shown in Figure 1. The figure shows the experimental results of case L=2. ‘+’, ‘o’ , ‘*’ , ‘△’ and ‘×’represent the estimated percentages of message capacity, corresponding to p=0.8, 0.6, 0.4,0.2, 0 . Figure 2 shows the distribution of the estimated embedding ratio (dashed lines are true ratios). The figure shows also only the experimental results of case L=2.

Because of the limited space, we do not show the experimental results of the case L=1, but the experimental results are as good as Fridrich's scheme.

VI. CONCLUSION

An extended detection method of LSB steganography has been formulated in this paper. To evaluate the proposed steganalytic method, four examples of estimation have been performed. It is shown that the accuracy of estimating the embedding ratio of secret messages is relatively high. Experimental results and theoretical verification have shown that this mehod is an effective steganlytic method of LSB stegaography.

REFERENCES

[1] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. [1] C. K. Chan, and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, Volume 37, Issue 3, pp.469-474, 2004.

[2] E. Kawaguchi and R. O. Eason, "principle and applications of BPCS-Steganography, " In Proceedings of SPIE: Multimedia Systems and Applications, vol.3528, pp. 464–472, 1998.

[3] Steganography software for Windows, http://members.tripod.com/steganography/ stego/software.html.

[4] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images," Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, pp. 22–28, 2001.

[5] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis," In IEEE transactions on signal Processing, Volume.51, Issue 7, pp.1995- 2007, July 2003.

[6] J. Fridrich, M. Goljan, "On Estimation of Secret Message Length in LSB Steganography in Spatial Domain," In Proceedings of EI SPIE Electronic Imaging, San Jose, CA, Jan. 2004.

[7] T. Zhang, X. Ping, "Reliable Detection of LSB Steganography Based on Difference Image Histogram," In Proceedings of ICASSP, vol. I, pp.545-548, 2003.

[8] X. Zhang, S. Wang, K. Zhang, "Steganography with least histogram abnormality," In: Lecture Notes in Computer Science, vol. 2776, pp. 395-406, 2003.

[9] X. Yu, T. Tan and Y. Wang, "Isotropy-Based Detection and Estimation: A General Framework of LSB Steganalysis," submitted to IEEE Trans. on Image Processing.

[10] M. Niimi, R. O. Eason, H. Noda, E. Kawaguchi, "Intenisty histogram steganalysis in BPCS-steganography," In Proceedings of SPIE, Security and Watermarking of Multimedia Contents, Vol.4314, pp.555-564, Electronic Imaging 2001 San Jose, 20-26 January, 2001.

[11] Corel Image Database, http://abacus.ee.cityu.edu.hk/~benjiman/corel_1/