Chinese Journal of Electronics
Vol.18, No.2, Apr. 2009

# Detecting LSB Steganography Based on Noise Function*

NIU Shaozhang[1], ZHOU Qi[2], CUI Baojiang[1] and ZHOU Linna[3]

(1.*National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China* )

(2.*Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China* )

(3.*Department of Electronic Engineering, Tsinghua University, Beijing 100084, China*)

**Abstract — This paper presents ND (Noise function detection) steganalysis algorithm to detect LSB steganography. The purpose of constructing the noise function is to quantify the smoothness or "regularity" of the images. ND method is based on the property that LSB embedding will increase the noise functional value of the image, and then the LSB embedding message ratio is estimated by constructing the simple line equation with the statistics of noise function in image. Experimental results show that this algorithm is more accurate and has a lower missing rate and false alarm rate than the conventional RS. Compared with RS method and some other powerful steganalysis approaches presented recently, ND method directly use the noise function to estimate the LSB embedding message ratio, neither fixed nor dynamic mask is needed. Thus, more running time is saved. The ND method is relatively faster, simpler and has good detection result.**

**Key words — Information hiding, Least significant bit (LSB) embedded, Steganography detection.**

## I. Introduction

The computer and network technology bring a lot of conveniences, but at the same time, they also give a great challenge to the information security technology. Steganography is the art of secret communication. Its purpose is to convey messages secretly by concealing the very existence of messages under digital media files[1]. Compared with the cryptography, steganography not only encrypts messages but also masks the very presence of the communication. We can use digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as covers or carriers to hide secret messages. After embedding a secret message into the cover image, we obtain a so-called stego image. It's important that the stegoimage not contain any detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once a third party can reliably identify which images contain secret messages, the steganographic tool becomes useless. Although by no means the most secure method of embedding data in images, LSB steanography tools are now extremely widespread. Therefore, it's of great significance to detect the images with hidden messages produced by LSB embedding effectively, accurately and reliably.

Westfeld[2] proposed a method based on statistical analysis of Pairs of values (PoVs) that are exchanged during message embedding. This method gives a successful result to a sequential LSB (Least significant bit) embedding steganography. However, randomly scattered messages can only be reliably detected with this method when the message length becomes comparable with the number of pixels in the image. Fridrich *et al.*[3,4] described a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. This method counts the number of regular and singular groups respectively, describes the RS chart, and constructs a quadratic equation. Then the ratio of message embedded in image can be estimated by solving this equation. However, there are three main factors that influence the accuracy of the estimated message length: the initial bias, the noise level or quality of the cover image, and the placement of message bits in the image. The assignment of flipping to pixels can be captured with a mask $M$, they detected the number of pixels with flipped LSBs in each stego image using their method. Andrew Ker[5,6] proposed the Improvement RS (IRS) method via experiment and pointed out that estimating the embedding ratio based on the statistics of regular groups in image only was more accurate. Being enlightened by RS steganalysis and Ker's improvement method, Xiangyang Luo *et al.*[7] developed a DRS (Dynamic regular groups steganalysis) algorithm. This algorithm constructs the embedding ratio-estimate equations only via regular groups and chooses an appropriate mask dynamically for each image to reduce the initial bias.

This paper presents ND (Noise function detection) steganalysis algorithm to detect LSB steganography. Experimental results show that this algorithm is more accurate and has a

*Manuscript Received Aug. 2008; Accepted Oct. 2008. This work is supported by the National High Technology Research and Development Program of China (863 Program) (No.2007AA01Z466, No.2008AA011004).

lower missing rate and false alarm rate than the conventional RS, IRS, and DRS method. At the same time, the ND method is relatively faster, simpler and has good detection result. In Section II, we review the principle of RS steganalysis, then in Section III describe the principle of ND algorithm. In Section IV, we give the detailed step noise detect algorithm. Section V shows the experimental results and we conclude this paper in Section VI.

## II. Principle of LSB Steganalysis

In the simple LSB steganography, the hidden message is converted to a stream of bits which replace the LSBs of pixel values in the cover image. When the hidden message contains less bits than the cover image has pixels, we assume that the modifications are spread randomly around the cover image according to a secret key shared with the intended recipient of the stego image. One should clearly distinguish this method (perhaps best called LSB replacement) from an alternative described in Ref.[8], where the cover pixel values are randomly incremented or decremented so that the least significant bits match the hidden message (this should perhaps be called LSB matching). In the latter case the message is still conveyed using the LSBs of the pixel values of the image, but the simple alteration to the embedding algorithm makes it much harder to detect.

Many methods for LSB Steganalysis have been proposed[2−7]. Fridrich *et al.* presented the powerful RS method (Regular and singular groups method) for detection of LSB embedding that utilizes sensitive dual statistics derived from RS correlations in images. Then, some improved RS methods were developed by Andrew Ker[5,6] and Xiangyang Luo[7]. But the main idea of the steganalysis algorithms is unchanged.

The RS steganalysis algorithm is based on the partition of an image's pixels as three disjoint groups: regular, singular and unusable groups. To explain the details of RS steganalysis, we need to define some notations. Assume that we have a cover image $C$ with $M \times N$ pixels and with pixel values from the set $P$. For example, for an 8-bit grayscale image, $P = \{0, \cdots, 255\}$. The stego-detection method starts with dividing the image into disjoint groups of $n$ adjacent pixels $G = (x_1, \cdots, x_n)$. We define so called discrimination function $f$ that assigns a real number $f(x_1, \cdots, x_n) \in R$ to each pixel group $G = (x_1, \cdots, x_n)$ as follows:

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

The invertible operation $F$ on $P$ called flipping is also defined.

$$F_1 : 0 \leftrightarrow 1, 2 \leftrightarrow 3, \cdots, 254 \leftrightarrow 255;$$
$$F_{-1} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, 3 \leftrightarrow 4, \cdots, 253 \leftrightarrow 254, 255 \leftrightarrow 256;$$
$$F_{-1}(x) = F_1(x+1) - 1 \quad \text{for all} \quad x.$$

For completeness, we also define $F_0$ as the identity permutation $F(x) = x$ for all $x \in P$. Then the group $G$ is dependent on one of the three types of pixel group.

Regular groups: $G \in R \Leftrightarrow f(F(G)) > f(G)$

Singular groups: $G \in S \Leftrightarrow f(F(G)) < f(G)$

Unusable groups: $G \in U \Leftrightarrow f(F(G)) = f(G)$,

For any mask $M$, $F_M(F_{M(1)}(x_1), F_{M(2)}(x_2), \cdots, F_{M(n)}(x_n))$ is also dependent on one of types in the $R$, $S$ and $U$. Fridrich experimentally verified the following two statistical assumptions with a large database of images which are unprocessed raw BMPs, JPEGs, and processed BMP images.

$$R_M + S_M \leq 1 \quad \text{and} \quad R_{-M} + S_{-M} \leq 1$$
$$R_M \cong R_{-M} \quad \text{and} \quad S_M \cong S_{-M}$$
$$R_M(1/2) = S_M(1/2)$$

where the mask $M$ denotes $M = [\,F_0 \quad F_1;\quad F_1 \quad F_0\,]$ and $-M$ denotes $-M = [\,F_0 \quad F_{-1};\quad F_{-1} \quad F_0\,]$. By randomizing the LSB plane of the stego image, we can obtain the middle points $R_M(1/2)$ and $S_M(1/2)$. Through an extensive of experiments, Fridrich got the estimate of RS-diagram, it possible to derive a ratio-estimate equation to calculate the embedding ratio $p$. Groups of $2 \times 2$ pixels with the mask [1 0; 0 1] (RS1) and [0 1; 1 0] (RS2) were used in their experiment.

Andrew Ker investigated a number of other masks and found that a performance improvement could be obtained using the square [0, 0, 0; 0, 1, 0; 0, 0, 0] instead the mask [0, 1, 1, 0] or [1, 0; 0; 1] used in conventional RS steganalysis. Xiangyang Luo *et al.* developed a dynamic regular groups steganalysis algorithm to detect LSB steganography. This algorithm dynamically selects an appropriate mask for each image to reduce the initial bias, and estimates the LSB embedding message ratio by constructing equations with the statistics of regular groups in image. DRS algorithm is more accurate than RS except for running time.

All these algorithms use mask time after time for the stego image, and more time is needed. Next, we use the discrimination function directly for LSB steganalysis.

## III. Principle of ND Steganalysis

The purpose of the discrimination function is to quantify the smoothness or "regularity" of the stego image. The noisier the stego image is, the larger the value of the discrimination function (best called noise function) becomes.

A cover grayscale image $C$ with $M \times N$ pixels corresponds to a nonnegative matrix $C = (c_{ij})_{M \times N}$ (all the elements of $C$ are nonnegative). We define the noise function of $C$ as smoothness of the stego image in rows and columns.

$$f(C) = \sum_{i=1}^{M} \sum_{j=1}^{N-1} |c_{i,j+1} - c_{ij}| + \sum_{j=1}^{N} \sum_{i=1}^{M-1} |c_{i+1,j} - c_{ij}|$$

We will study the possibility of estimating the initial bias from stego images to improve the sensitivity of the ND method. Although we know that value of the noise function becomes larger after embedding, we need more experiments to obtain the value of the noise function for different images.

We apply random LSB replacement to embed the images with the ratio of $p = 0$, 3%, 5%, 10%, 20%, $\cdots$, 90%, 100% respectively, and so we do LSB matching. Their diagrams appear in Fig.1 and Fig.2.

We have collected experimental evidence that the noise functions of image are well modeled with straight lines. These have been experimentally verified for the above two images and a large database of images with unprocessed raw BMPs, JPEGs, and processed BMP images. The parameters of the curves can be determined from the two points marked in Fig.1. They make it possible to derive a simple formula for the secret message ratio $p$. First, we calculate the value $f(C)$, and let $v_1 = f(C)$. Then if we know the noise functional values $v_2$ and $v_3$ with the embedding ratio 100% and 0% respectively, the message ratio $p$ is calculated from the straight line as

$$p = (v_1 - v_3)/(v_2 - v_3).$$

To estimate the noise functional values $v_2$, we use random LSB replacement again to embed the images with the ratio of $p = 0$, 3%, 5%, 10%, 20%, $\cdots$, 90%, 100% respectively for the random LSB replacement stego images with the ratio of 0, 3%, 5%, 10%, 20%, $\cdots$, 90% , 100%. The result, typical for images with the maximal embedding ratio close to fix value, is plotted in Fig.3.

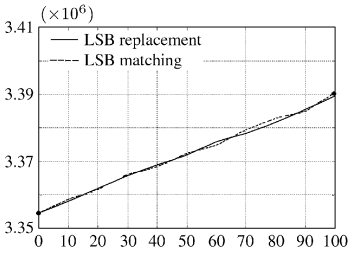


Fig. 1. The noise function of Peppers.bmp

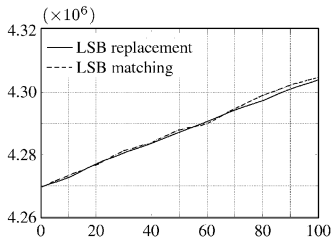


Fig. 2. The noise function of Sailboat.bmp

As can be seen from the chart, the noise functional value with the maximal embedding ratio is unchanged for the random LSB replacement. Theoretical analysis also shows this property since the randomicity of LSBs of the image becomes better with the increasing on the embedding ratio. From this result, we can estimate the value $v_2$ by applying random LSB replacement again to embed the stego images with the ratio of 100%. However, this property is not held for LSB matching, and so we only discuss random LSB replacement.

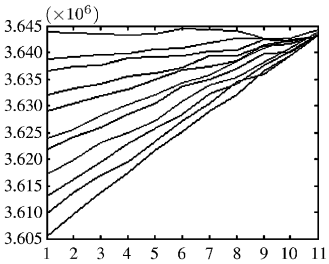


Fig. 3. Apply LSB replacement again for the stego image

For each natural image, all horizontally and vertically adjacent Pairs of pixels in the image include the following three cases.

**Case 1** The LSBs of two adjacent Pairs are equal;

**Case 2** The LSBs of two adjacent Pairs are not equal, but the LSB of pixel with bigger value is 0, and the other one is 1;

**Case 3** The LSBs of two adjacent Pairs are unequal, but the LSB of pixel with bigger value is 1, and the other one is 0.

We suppose that the numbers of adjacent Pairs in Case 2 and Case 3 are equal. The assumption makes it possible to derive that the noise functional value of a natural image approximates to its noise functional value with replacing all LSBs of the image with zeros. We experimentally verified these assumptions for a large database of images with unprocessed raw BMPs. Due to space limitations, we omit the theoretical proof.

There are several factors that influence the accuracy of the estimated message length. But in order to get the most accurate estimate of embedding ratio, we can repeatedly enumerate the parameter $v_2$ and use their average value.

## IV. Description of ND Algorithm

Now we describe our detection algorithm as follows.

**Input** A BMP image $C$ for detecting.

**Output** The embedding ratio $p$ of the image $C$.

**Step 1** Calculate the value $f(C)$, and let $v_1 = f(C)$;

**Step 2** Apply random LSB replacement to embed the image $C$ with the ratio of 100%, then obtain value $f(C)$ and denote $v_2 = f(C)$;

**Step 3** Replace all LSBs of the image $C$ with zeros, compute the value $f(C)$ and get $v_3 = f(C)$;

**Step 4** Find out the embedding ratio $p$ of the image $C$.

$$p = (v_1 - v_3)/(v_2 - v_3)$$

## V. Experimental Results and Analysis

Similar to RS algorithm, there exists some initial bias in ND algorithm. Even original cover-images may indicate a small non-zero message length due to random variations. This initial non-zero bias could be both positive and negative and it puts a limit on the achievable accuracy of our steganalysis.

We select 8 standard $512 \times 512$ or $256 \times 256$ (such as Lena, Peppers and so on) to test this initial bias. The mask used in the RS method and IRS method is [1,0; 0,1] (RS1), [1 0; 0 1] (RS1) and [0 1; 1 0] (RS2) (RS2) and [0,0,0; 0,1,0; 0,0,0] respectively. Table 1 shows the test result.

**Table 1. Initial bias**

| Images | RS1 | RS2 | IRS | ND |
|---|---|---|---|---|
| Lena256.bmp | −0.439% | −1.46% | −1.32% | −1.25% |
| Lena.bmp | −1.21% | −2.02% | −1.30% | −1.75% |
| Couple.bmp | −0.0009% | 0.173% | −1.12% | 0% |
| Girl.bmp | −0.07% | 0.0519% | −0.714% | 0% |
| Airplane.bmp | 1.59% | 1.54% | 1.27% | 2.30% |
| Peppers.bmp | 1.30% | 0.858% | 0.721% | 0.80% |
| Sailboat.bmp | 0.787% | −0.765% | 1.10% | 1.00% |
| Baboo.bmp | 3.046% | 0.043% | 1.96% | 2.79% |

To demonstrate the testing results in details, we give the test embedding ratio of these four images (Lena, Peppers, Sailboat and Baboo) one by one instead of their average values. Applying random LSB replacement to embed these images with the ratio of $p = 0$, 3%, 5%, 10%, 20%, $\cdots$, 90% respectively, and then use ND method to estimate the embedding ratio of secret information. The testing results of ND method are given in Table 2. The leftmost column in Table 2 is the real embedding ratio, and column “Lena”, “Peppers”, “Sailboat”

and "Baboo" represent the estimate embedding ratio got by ND method.

**Table 2. The testing results of ND method**

| | Lena | Peppers | Sailboat | Baboo |
|---|---|---|---|---|
| 0 | −1.75 | 0.80 | 1 | 2.79 |
| 3 | 1.53 | 3.94 | 3.86 | 3.34 |
| 5 | 3.65 | 6.31 | 6.01 | 5.32 |
| 10 | 7.48 | 11.73 | 12.69 | 16.29 |
| 20 | 19.5 | 20.34 | 19.24 | 23.17 |
| 30 | 31.32 | 31.07 | 30.30 | 30.24 |
| 40 | 38.98 | 45.27 | 43.16 | 43.32 |
| 50 | 51.05 | 48.16 | 52.85 | 49.46 |
| 60 | 59.57 | 60.63 | 60.97 | 62.79 |
| 70 | 70.98 | 69.25 | 69.87 | 73.91 |
| 80 | 82.99 | 80.29 | 83.87 | 79.63 |
| 90 | 88.82 | 89.78 | 90.79 | 94.44 |

It can be seen in Table 2 that the estimate precision of ND is much effective for random LSB replacement. But we also recognize that the precision is discrepant for different images, especially for Baboo, in which there may be more textures. The precision has something to do with the image itself. The comparison of correct ratio of RS, IRS, SPA and DRS method is given in Ref.[7]. However, the precision in Ref.[7] is the average value of 50 standard $512 \times 512$ test images (such as Lena, Peppers and so on), not of single image. The precision degree of ND is higher than RS when the embedding ratio is lower than 10%. According to the average, the ND method is more accurate. In general, the ND method gives us wonderful and accurate detections for stego images. Comparing with to RS, IRS, and DRS, we need neither fixed nor dynamic Mask in the ND method. Thus, more running time is saved.

## VI. Conclusions

This paper presents ND (Noise function detection) steganalysis algorithm to detect LSB steganography. ND estimates the ratio of embedding message by constructing the discrimination function, which is to quantify the smoothness or "regularity" of the images. Our method is based on the property that LSB embedding will increase the noise functional value of the image, and then we can estimate the LSB embedding message ratio by constructing the simple line equation with the statistics of noise function in image. ND method directly uses the noise function to estimate the LSB embedding message ratio, neither fixed nor dynamic Mask is needed. Hence, ND method is faster and simpler than the conventional RS method. Experimental results show that ND steganalysis method is more accurate and has a lower missing and false alarm rate than the conventional RS method.

The subject of our future research will be focused on studying the possibility of constructing more exact equations from stego images to improve the sensitivity of the ND detection method. We will also study on applying the ND detection to LSB matching steganography.

### References

[1] R.J. Andersen and F.A.P. Petitcolas, "On the limits of steganography", *IEEE J. Selected Areas in Comm.*, Vol.16, No.4, pp.474–481, 1998.

[2] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems", *Lecture Notes in Computer Science*, Vol.1768, Springer-Verlag, Berlin, pp.61–75, 2000.

[2] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems", *Proc. 3rd Information Hiding Workshop*, Dresden, Germany, Sept. 28-Oct. 1, pp.61–75, 1999.

[3] J. Fridrich, M. Goljan, R. Du, "Reliable detection of LSB steganography in color and grayscale image", In *Proc. of the ACM Workshop on Multimedia and Securtity*, Dttawa: ACM Press, pp.27–30, 2001.

[4] J. Fridrich, M. Goljan, "Practical steganalysis of digital images-state of the art", In Delp III, E.J., Wong, P.W., eds.: *Security and Watermarking of Multimedia Contents IV*, Vol.4675 *of Proc. SPIE*. pp.1–13, 2002.

[5] Andrew D. Ker, "Quantitive evaluation of pairs and rs steganalysis", In Delp III, E.J., Wong, P.W., eds.: *Security, Steganography, and Watermarking of Multimedia Contents VI*. Vol.5306 *of Proc. SPIE*, pp.83–97, 2004.

[6] Andrew D. Ker, "Improved detection of LSB steganography in grayscale images", *Proc. The 6th Information Hiding Workshop*. Vol.3200 *of Springer LNCS*, pp.97–115, 2004.

[7] Luo Xiangyang, Liu Bin, Liu Fenlin, "Detecting LSB steganography based on dynamic masks", *Intelligent Systems Design and Applications, 2005. ISDA '05. Proceedings. 5th International Conference*, pp.251–255, 2005.

[8] T. Sharp, "An implementation of key-based digital signal steganography", In: *Proc. Information Hiding Workshop*, Vol.2137 *of Springer LNCS*, pp.13–26, 2001.

**NIU Shaozhang** was born in 1963, Ph.D., professor. His main research interests include information hiding, steganalysis, digital forensic, network and information security, technology for disaster backup and recovery.

**ZHOU Qi** received B.S. degree in 2006. He is now a dual M.S. degree student majoring in computer software and theory in Shanghai Jiaotong University and electrical and computer engineering in Georgia Institute of Technology respectively.

**CUI Baojing** was born in 1973, associate professor, supervisor of Ph.D. candidate, research area inclndes network and information security, software security and remote disaster tolerance.

**ZHOU Linna** was born in 1972, Ph.D., she is currently a software engineer in digital forensic, watermarking, cryptology and multimedia content security.