Equivalence Analysis among DIH, SPA, and RS Steganalysis Methods

Xiangyang Luo, Chunfang Yang, Fenlin Liu

Information Engineering University, Zhengzhou, China.
xiangyangluo@126.com

Abstract. steganography of images based on the use of the LSB (Least Significant Bit), SPA (Sample Pair Analysis), RS (Regular and Singular groups) method and DIH (Difference Image Histogram) method are three powerful steganalysis methods. A comparison analysis among DIH, SPA, and RS method is discussed, and a comparison of their proofs is presented. The process of proving includes three parts, and an equivalence relationship proposition is respectively proofed in every section. This proving offers a theory base for the study of an approach that can resist these three kinds of steganalysis methods synchronously.

1 Introduction

Steganography is one of the important research subjects in information security field. As a new art of covert communication, the main purpose of steganography is to convey messages secretly by concealing the very existence of messages under digital media files, such as images, audio, or video files. Similar to encryption and cryptanalysis, steganalysis attempts to defeat the goal of steganography. It is the art of detecting the existence of the secret message. Steganalysis finds applications in cyber warfare, computer forensics, tracking criminal activities over the Internet and gathering evidence for investigation. Steganalysis is also practiced for evaluating, identifying the weaknesses, and improving the security of steganographic systems.

Among the many steganographic methods involving images, LSB Steganography tools are now extremely widespread because of fine concealment, great capability of hidden message and easy realization. Making the detection of LSB steganography effective and reliable is a valuable topic for communication and multimedia security. Presently, there are some powerful LSB steganalysis methods, such as χ^2–statistical analysis[1], SPA method[2][3], RS steganalysis[4][5], DIH steganalysis[6][7][11] and so on. SPA steganalysis can detected the LSB steganography via sample pairs analysis. When the embedding ratio is more than 3%, it can estimate the embedding ratio with relatively high precision, and the average estimation error is 0.023. We improved SPA method, and proposed a more accurate LSB steganalysis method, called LSM (least square method) steganalysis in paper [8].

RS method, suitable for color and gray-scale images, is based on the number of the regular group and the singular one, and constructs a quadratic equation.

The embedding ratio of message in image is then estimated by solving the equation. This method can accurately estimate the length of the embedded messages when they are embedded randomly. An improved RS method based on dynamic masks is present in paper [9], which dynamically selects an appropriate mask for each image to reduce the initial deviation, and estimates the LSB embedding ratio more accurately. In addition, Andrew D. Ker [10] estimated the reliabilities of RS and SPA through a large number of experiments, and proposed some good improvement measures.

T. Zhang et al. [6][7][11] introduced a steganalytic method for detection of LSB embedding via different histograms of image, named DIH method. When the embedding ratio is more than 40% or less than 10%, the result is more accurate than that of RS method, and the speed of this method is faster.

In this paper, an equivalence analysis among DIH, SPA and RS method is discussed, and an equivalence proving of these three kinds of methods is presented. The proving process includes three parts, and three propositions are respectively proofed in these parts.

2 Principle of DIH, SPA, and RS Method

In this section, we simply describe the principle of DIH, SPA and RS method as a base of the equivalence proving.

2.1 Principle of DIH Method

A digital image can be represented by a set of pixels $s_1, s_2, \cdots, s_N$, where the index corresponds to the position of each pixel, and $\tilde{s}_k$ denotes the pixel adjacent to s_k (we consider adjacency in both dimensions, even though the indexes are not sequential). T. Zhang et al.[11] defines the pixel sets as follows:

$$H_n = \{s_k | s_k - \tilde{s}_k = n, k = 1, 2, \cdots, N, 0 \leq n \leq 255\} \tag{1}$$

$$G_{2m} = \{s_k | int\,(s_k/2) - int\,(\tilde{s}_k/2) = m, k = 1, 2, \cdots, N,\ 0 \leq m \leq 127\} \tag{2}$$

where $int\,(x)$ is the maximal integer that are not larger than x. Based on the relationship between G_{2m} andH_n, the following partition of G_{2m} can be obtained:

$$G_{2m} = A_{2m-1} \cup H_{2m} \cup B_{2m+1} \tag{3}$$

where

$$\begin{cases} A_{2m-1} = H_{2m-1} \cap G_{2m} = \{s_k | s_k \in G_{2m}, s_k \bmod 2 = 0, \tilde{s}_k \bmod 2 = 1, k = 1, \cdots, N\} \\ H_{2m} = H_{2m} \cap G_{2m} = \{s_k | s_k \in G_{2m}, (s_k \bmod 2) = (\tilde{s}_k \bmod 2), k = 1, \cdots, N\} \\ B_{2m+1} = H_{2m+1} \cap G_{2m} = \{s_k | s_k \in G_{2m}, s_k \bmod 2 = 1, \tilde{s}_k \bmod 2 = 0, k = 1, \cdots, N\} \end{cases} . \tag{4}$$

Namely, for every s_k in A_{2m-1}, there is an adjacent pixel$\tilde{s}_k$, $s_k - \tilde{s}_k = 2m-1$, and $int\,(s_k/2) - int\,(\tilde{s}_k/2) = m$; for every s_k in B_{2m+1}, there is an adjacent pixel $\tilde{s}_k$, $s_k - \tilde{s}_k = 2m+1$, and $int\,(s_k/2) - int\,(\tilde{s}_k/2) = m$.

Define the transfer coefficient among the difference image histograms as follows:

$$a_{2m,2m-1} = \|A_{2m-1}\|/\|G_{2m}\|, \quad a_{2m,2m} = \|H_{2m}\|/\|G_{2m}\|,$$
$$a_{2m,2m+1} = \|B_{2m+1}\|/\|G_{2m}\| \tag{5}$$

where $\|\bullet\|$ denotes the cardinality of set $\bullet$. For $j = 0, \ \pm 1$, $0 < a_{2m,2m+j} < 1$ or $a_{2m,2m+j} = 0$, and

$$a_{2m,2m-1} + a_{2m,2m} + a_{2m,2m+1} = 1. \tag{6}$$

DIH method denotes $h_m = \|H_m\|$, $g_{2m} = \|G_{2m}\|$ and f_m as the difference histograms of the detected image, the image in which after the LSB of every pixel is set as 0 and the image in which after the LSB of every pixel is flipped.

According to the definition of h_{2m+1}, it is known that h_{2m+1} comprises of $a_{2m,2m+1}g_{2m}$ and $a_{2m+2,2m+1}g_{2m+2}$.A majority of statistical tests show that for the natural images these two parts make an approximately equal contribution to h_{2m+1}, i.e.

$$a_{2m,2m+1}g_{2m} \approx a_{2m+2,2m+1}g_{2m+2}. \tag{7}$$

DIH method notes that $\alpha_m = a_{2m+2,2m+1}/a_{2m,2m+1}$, $\beta_m = a_{2m+2,2m+3}/a_{2m,2m-1}$ and $\gamma_m = g_{2m}/g_{2m+2}$, and makes the statistical hypothesis that satisfies

$$\alpha_m \approx \gamma_m, \tag{8}$$

For the natural image; but for the stego-images with LSB plane fully embedded, it satisfies

$$\alpha_m \approx 1. \tag{9}$$

Literature [6][11] selects the quadratic polynomial to simulate the relationship between α_m and p, and utilizes four key points $P_1 = (0, \gamma_m)$, $P_2 = (p, \alpha_m)$, $P_3 = (1, 1)$ and $P_4 = (2 - p, \beta_m)$ to obtain the estimation equation:

$$2d_1p^2 + (d_3 - 4d_1 - d_2)p + 2d_2 = 0 \tag{10}$$

Where $d_1 = 1 - \gamma_m$, $d_2 = \alpha_m - \gamma_m$ and $d_3 = \beta_m - \gamma_m$. DIH regards the root of equation (10) whose absolute value is smaller as the estimate value of the embedding ratio p.

2.2 Principle of SPA Method

S. Dumitrescu et al.[2] denotes a pair of pixels as a two-tuple $(s_i, s_j), 1 \le i, j \le N$, where N is the total number of pixels of an image. Then an estimation equation of the embedding ratio is based on the following important hypothesis:

$$E\left\{\|X_{2m+1}\|\right\} = E\left\{\|Y_{2m+1}\|\right\}, \tag{11}$$

where X_{2m+1} is the multiset consisting of the adjacent pixel pairs, for each (s_i, s_j) in X_{2m+1}, $|s_i - s_j| = 2m+1$ and the even component in X_{2m+1} is larger; Y_{2m+1} is also the multiset consisting of the adjacent pixel pairs, for each (s_i, s_j) in Y_{2m+1}, $|s_i - s_j| = 2m+1$ and the odd component in Y_{2m+1} is larger.

The other important multisets are defined in paper [2], such as C_m, D_n, where C_m is the multiset consisting of the adjacent pixel pairs whose values differ by m in the first $b-1$ bits (b is the number of bits to represent each pixel value) (i.e., by right shifting one bit and then measuring the difference), and D_n is the multiset that consists of the adjacent pixel pairs whose values differ by n. The D_{2m+1} can be partitioned into two submultiset X_{2m+1} and Y_{2m+1}, and they satisfy $X_{2m+1} = D_{2m+1} \cap C_{m+1}$, $Y_{2m+1} = D_{2m+1} \cap C_m$, $0 \le m \le 2^{b-1} - 2$, and $X_{2^b-1} = \phi$, $Y_{2^b-1} = D_{2^b-1}$.

Considering the estimating precision, the literature [2] uses the hypothesis

$$E\left\{\left|\bigcup_{m=i}^{j} X_{2m+1}\right|\right\} = E\left\{\left|\bigcup_{m=i}^{j} Y_{2m+1}\right|\right\} \tag{12}$$

to replace (11), and then derives a more robust quadratic equations to estimate$p$.

2.3 Principle of RS Method

RS method partitions an image into $\lceil \frac{N}{n} \rceil$ groups of n adjacent pixels, where N is the total number of pixels in an image. In [5], the authors considered the case of$n = 4$. A discrimination function $f(\bullet)$ captures the smoothness of a group of pixels; and, we define three invertible operations$F_n(x)$, $n = -1, 0, 1$ on a pixel$x$, where F_1 and F_{-1} are applied to a group of pixel values through the mask M and$-M$. Mask$M$, an n-tuple with components 0 and 1, specifies where and how pixel values are to be modified;$-M$ is the n-tuple with the minus components of$M$,for example, if$M = (1, 0, 1, 0)$, then $-M = (-1, 0, -1, 0)$. Given a mask, operations F_1 andF_{-1}, and the discrimination function$f$, a pixel group G can be classified into one of the three categories described below:

$$\begin{aligned} G \in R(M) &\Leftrightarrow f(F(G)) > f(G) \\ G \in S(M) &\Leftrightarrow f(F(G)) < f(G) \\ G \in U(M) &\Leftrightarrow f(F(G)) = f(G) \end{aligned} \tag{13}$$

Where$R(M)$, $S(M)$ and $U(M)$ are respectively called Regular, Singular, and Unusable Groups. RS method is based on the statistical hypothesis that when no message is embedded in an image, the following equations hold:

$$E\{\|R(M)\|\} = E\{\|R(-M)\|\} \tag{14}$$

$$E\{\|S(M)\|\} = E\{\|S(-M)\|\}. \tag{15}$$

RS method builds a quadratic equation to estimate the embedding ratio p based on above-mentioned hypotheses (14) and (15), and the coefficients of the equation can be obtained by counting the number of Regular and Singular Groups with mask M and $-M$ in the examined image.

3 Comparison among DIH, SPA and RS Method

In this section, the comparative analysis among DIH, SPA and RS method will be given to prove their equivalence.

3.1 Equivalence between DIH and SPA Method

Proposition 1: The hypothesis (7) of DIH method is equivalent to the hypothesis (11) of SPA method.

Prove:

From equation (5), the following equations can be obtained:

$$a_{2m,2m+1}g_{2m} = (\|B_{2m+1}\|/\|G_{2m}\|)\,\|G_{2m}\| = \|B_{2m+1}\|\,,$$

$$a_{2m+2,2m+1}g_{2m+2} = (\|A_{2m+1}\|/\|G_{2m+2}\|)\,\|G_{2m+2}\| = \|A_{2m+1}\|\,.$$

Thus, the hypothesis (7) of DIH method can be converted into

$$\|A_{2m+1}\| = \|B_{2m+1}\|\,. \tag{16}$$

From (1), we can denote H_n as a set of pixel s_k whose value is larger than that of an adjacent pixel $\tilde{s}_k$ by$n$. And D_n is a set of all pairs of adjacent pixels whose values differ by$n$. Thus, the adjacent pixels s_k and $\tilde{s}_k$ whose values differ by n are the elements of H_n and H_{-n} respectively, and the pixel pairs $(s_k, \tilde{s}_k)$ and $(\tilde{s}_k, s_k)$ are both the elements ofD_n. Therefore, the result of$H_n \cup H_{-n}$ is D_n.

From (2), we can denote G_{2m} as a set of pixel s_k whose value is larger than that of an adjacent pixel $\tilde{s}_k$ by n in the first $b-1$ bits. And C_m is a set of all pairs of adjacent pixels whose values differ by n in the first $b-1$ bits. So, the above adjacent pixels s_k and $\tilde{s}_k$ are respectively the elements of G_{2m} andG_{-2m}, and the pixel pairs $(s_k, \tilde{s}_k)$ and $(\tilde{s}_k, s_k)$ are the elements ofC_m. Thus, $G_{2m} \cup G_{-2m}$equalsC_m.

From (4), it follows: denote A_{2m+1} as a set of pixel s_k whose value is larger than that of an adjacent pixel $\tilde{s}_k$ by $2m+1$ and in the first $b-1$ bits s_k is larger than $\tilde{s}_k$ by$m+1$. And X_{2m+1} is a set of all pairs of adjacent pixels whose values differ by $2m+1$ and $m+1$ in the first $b-1$ bits. Hence, the above adjacent pixels s_k and $\tilde{s}_k$ are the elements of A_{2m+1} and A_{-2m-1} respectively, and the pairs $(s_k, \tilde{s}_k)$ and $(\tilde{s}_k, s_k)$ are the elements of X_{2m+1}. Thereby, $A_{2m+1} \cup A_{-2m-1}$ is equivalent toX_{2m+1}.

As above, it follows: denote B_{2m+1} as a set of pixel s_k whose value is larger than that of an adjacent pixel $\tilde{s}_k$ by $2m+1$ and s_k is larger than $\tilde{s}_k$ by m in the first $b-1$ bits. And Y_{2m+1} is a set of all pairs of adjacent pixels whose values differ by $2m+1$ and m in the first $b-1$ bits. Therefore, the above adjacent pixels s_k and $\tilde{s}_k$ are the elements of B_{2m+1} and B_{-2m-1} respectively, and the pixel pairs $(s_k, \tilde{s}_k)$ and $(\tilde{s}_k, s_k)$ are the elements ofY_{2m+1}. Thus, $B_{2m+1} \cup B_{-2m-1}$ is equivalent to Y_{2m+1}.

If an arbitrarys_k belongs to H_n, G_{2m}, A_{2m+1} or B_{2m+1}, there must be a corresponding adjacent element $\tilde{s}_k$ belonging to H_{-n}, G_{-2m}, A_{-2m-1} or B_{-2m-1} respectively and vice versa. Consequently, it is held that

$$\|H_n\| = \|H_{-n}\|, \quad \|G_{2m}\| = \|G_{-2m}\|,$$
$$\|A_{2m+1}\| = \|A_{-2m-1}\|, \quad \|B_{2m+1}\| = \|B_{-2m-1}\|,$$

That is,

$$\|H_n\| = \frac{1}{2}\left(\|H_n\| + \|H_{-n}\|\right), \quad \|G_{2m}\| = \frac{1}{2}\left(\|G_{2m}\| + \|G_{-2m}\|\right),$$

$$\|A_{2m+1}\| = \frac{1}{2}\left(\|A_{2m+1}\| + \|A_{-2m-1}\|\right), \quad \|B_{2m+1}\| = \frac{1}{2}\left(\|B_{2m+1}\| + \|B_{-2m-1}\|\right). \tag{17}$$

In brief, DIH and SPA method adopt different means to build estimation equations: DIH method utilizes the similarity degree $\alpha_m = a_{2m+2,2m+1}/a_{2m,2m+1}$ between A_{2m+1}/B_{2m+1} and g_{2m}/g_{2m+2}, the ratio between $a_{2m,2m+1}g_{2m}$ and $a_{2m+2,2m+1}g_{2m+2}$ in h_{2m+1}, to model the relationship between α_m and p; and SPA method constructs the estimation equation of p through the transform probability among states that the adjacent pixel pairs belong to before and after embedding. However, the assumption (7) of DIH method is equivalent to the assumption $E\left\{\|Y_{2m+1}\|\right\} = E\left\{\|X_{2m+1}\|\right\}$ of SPA method in nature. In fact, both of them are based on the same hypothesis: for an natural image, in the adjacent pixels differing by$2m+1$, their probabilities differing by m or $m+1$ are equal. Consequently, The combination of (7) in$m = 0, \ \cdots, \ j$,$\sum_{m=i}^{j} a_{2m,2m+1}g_{2m} = \sum_{m=i}^{j} a_{2m+2,2m+1}g_{2m+2}$, namely $\left\|\bigcup\limits_{m=i}^{j} A_{2m+1}\right\| = \left\|\bigcup\limits_{m=i}^{j} B_{2m+1}\right\|$, is equivalent to the assumption (12) of SPA method.

3.2 Equivalence between DIH and RS Method

Proposition 2: When$n = 2$,$m = 0, \ \cdots, \ 2^{b-1}-2$, the hypotheses (14) and (15) of RS method is equivalent to the combination of hypothesis (7) of DIH method.

Prove:

When$n = 2$, M can be one of the four cases:$(1, \ 0)$,$(0, \ 1)$, $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$. Consider the case $M = (1, \ 0)$, the process of prove is as follows.

When $M = (1, \ 0)$, the pixels s_k and $\tilde{s}_k$ are horizontally adjacent. Two pixelsets $H_{00,2m}$ and $H_{11,2m}$ are defined here, both of whichs_k is larger than $\tilde{s}_k$ by $2m$. Furthermore, the LSBs of s_k in $H_{00,2m}$ and its adjacent pixel $\tilde{s}_k$ are both zeros and the LSBs of s_k in $H_{11,2m}$ and its adjacent pixel $\tilde{s}_k$ are both ones. Applying $M = (1, \ 0)$ into the detecting image, all the horizontal adjacent pixel pairs in the image can be partitioned by two means: $R(M)+S(M)$ and$R(-M)+S(-M)$.

1. If the adjacent pixel pair $(s_k, \tilde{s}_k)$ belongs to $R(M)$, then s_k and $\tilde{s}_k$ are equivalent, or the larger s_k becomes more larger, or the smaller s_k becomes more smaller through applying the operation F_1 into s_k. Namely, $(s_k, \tilde{s}_k)$ may be under one of the below cases:

$$\begin{cases} s_k > \tilde{s}_k, \text{ if } s_k \bmod 2 = 0 \\ s_k < \tilde{s}_k, \text{ if } s_k \bmod 2 = 1 \\ s_k = \tilde{s}_k \end{cases}.$$

Therefore,s_k belongs to

$$\left(\bigcup_{m=1}^{2^{b-1}-1} A_{2m-1}\right) \cup \left(\bigcup_{m=1}^{2^{b-1}-1} A_{-2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} H_{00,2m}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} H_{11,-2m}\right).$$

Replacing m by $m+1$ in the above formula, it follows that

$$\left(\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right) \cup \left(\bigcup_{m=-1}^{2^{b-1}-2} H_{00,2m+2}\right) \cup \left(\bigcup_{m=-1}^{2^{b-1}-2} H_{11,-2m-2}\right),$$

Namely,

$$\left(\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right) \cup H_{00,0} \cup H_{11,0} \cup \left(\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}\right) \cup \\ \cup \left(\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}\right). \tag{18}$$

If s_k belongs to$\left(\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right) \cup H_{00,0} \cup H_{11,0}$, then its adjacent pixel $\tilde{s}_k$ must also belong to $\left(\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right) \cup H_{00,0} \cup H_{11,0}$ and $(s_k, \tilde{s}_k)$ must be of$R(M)$. If s_k belongs to$\left(\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}\right)$, then $(s_k, \tilde{s}_k)$ must be of$R(M)$, but $\tilde{s}_k$ must not be an element of $\left(\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}\right)$. Therefore,

$$\|R(M)\| = \frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right\| + \|H_{00,0}\| + \|H_{11,0}\|\right) \\ + \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}\right\| \tag{19}$$

1. If $(s_k, \tilde{s}_k)$ belongs to$R(-M)$, then s_k and $\tilde{s}_k$ are equivalent, or the larger s_k becomes smaller or the smaller s_k becomes larger through applyingF_1 into s_k. Namely, $(s_k, \tilde{s}_k)$ may be under one of the following cases:

$$\begin{cases} s_k > \tilde{s}_k, \text{ if } s_k \bmod 2 = 1 \\ s_k < \tilde{s}_k, \text{ if } s_k \bmod 2 = 0 \\ s_k = \tilde{s}_k \end{cases},$$

Similar to i), we can obtain

$$\|R(-M)\| = \tfrac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right\| + \|H_{00,0}\| + \|H_{11,0}\|\right) + \left\|\bigcup_{m=1}^{2^{b-1}-1} H_{11,2m}\right\| + \left\|\bigcup_{m=1}^{2^{b-1}-1} H_{00,2m}\right\| . \tag{20}$$

The proving process will be specified in Appendix.

1. If $(s_k, \tilde{s}_k)$ belongs to $S(M)$, then $(s_k, \tilde{s}_k)$ may be classified into two categories:

$$\begin{cases} s_k > \tilde{s}_k, \text{ if } s_k \bmod 2 \ = 1 \\ s_k < \tilde{s}_k, \text{ if } s_k \bmod 2 \ = 0 \end{cases} .$$

Similar to i) and ii), we can prove

$$\|S(M)\| = \frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right\|\right) + \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{11,2m+2}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{00,-2m-2}\right\| . \tag{21}$$

1. If $(s_k, \tilde{s}_k)$ belongs to $S(-M)$, $(s_k, \tilde{s}_k)$ may be classified into two classes:

$$\begin{cases} s_k > \tilde{s}_k, \text{ if } s_k \bmod 2 \ = 0 \\ s_k < \tilde{s}_k, \text{ if } s_k \bmod 2 \ = 1 \end{cases} .$$

Similar to i), we can obtain that

$$\|S(-M)\| = \frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right\|\right) + \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}\right\| + \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}\right\| . \tag{22}$$

From the definitions of A_{2m+1}, B_{2m+1}, $H_{00,2m}$ and $H_{11,2m}$, it can be shown that: if a arbitrary pixel s_k belongs to $\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}$, $\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}$, $\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}$ or $\bigcup_{m=0}^{2^{b-1}-2} H_{11,2m+2}$, then there must be only one adjacent $\tilde{s}_k$ belonging to $\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}$, $\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}$, $\bigcup_{m=0}^{2^{b-1}-2} H_{00,-2m-2}$ or $\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}$. Hence

$$\left\|\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right\| = \left\|\bigcup_{m=0}^{2^{b-1}-2} A_{-2m-1}\right\|, \quad \left\|\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right\| = \left\|\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right\|,$$

$$\left\|\bigcup_{m=0}^{2^{b-1}-2} H_{00,2m+2}\right\| = \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{00,-2m-2}\right\|,$$
$$\left\|\bigcup_{m=0}^{2^{b-1}-2} H_{11,2m+2}\right\| = \left\|\bigcup_{m=0}^{2^{b-1}-2} H_{11,-2m-2}\right\| . \tag{23}$$

Based on hypotheses (14) and (15), we can obtain

$$\begin{aligned}&\frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-2}A_{2m+1}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-2}A_{-2m-1}\right\|+\|H_{00,0}\|+\|H_{11,0}\|\right)\\&\qquad+\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{00,2m+2}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{11,-2m-2}\right\|\\&=\frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-1}B_{2m+1}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-1}B_{-2m-1}\right\|+\|H_{00,0}\|+\|H_{11,0}\|\right)\\&\qquad+\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{11,2m+2}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{00,-2m-2}\right\|\end{aligned}, \tag{24}$$

and

$$\begin{aligned}&\frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-1}B_{2m+1}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-1}B_{-2m-1}\right\|\right)+\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{11,2m+2}\right\|+\\&\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{00,-2m-2}\right\|=\frac{1}{2}\left(\left\|\bigcup_{m=0}^{2^{b-1}-2}A_{2m+1}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-2}A_{-2m-1}\right\|\right)+.\\&\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{00,2m+2}\right\|+\left\|\bigcup_{m=0}^{2^{b-1}-2}H_{11,-2m-2}\right\|\end{aligned} \tag{25}$$

From (23), (24) and (25), it can be further obtained that

$$\left\|\bigcup_{m=0}^{2^{b-1}-2}A_{2m+1}\right\|=\left\|\bigcup_{m=0}^{2^{b-1}-1}B_{2m+1}\right\|. \tag{26}$$

Usually, when $b = 8$, the probability of two adjacent pixels differing by 255, viz.$2^b - 1$, is nearly zero. As a result, (26) can be shown in the following way

$$\left\|\bigcup_{m=0}^{2^{b-1}-2}A_{2m+1}\right\|=\left\|\bigcup_{m=0}^{2^{b-1}-2}B_{2m+1}\right\|. \tag{27}$$

Accordingly, when $M = (1, 0)$, the assumptions (14) and (15) of RS method are equivalent to the combination of assumption (7) of DIH method.

In the same way, the equivalence relationship can be proofed when $M = (0, 1)$, $\begin{pmatrix}1\\0\end{pmatrix}$ or $\begin{pmatrix}0\\1\end{pmatrix}$.

To sum up, when $n = 2$, $m = 0, \cdots, 2^{b-1} - 2$, the assumptions (14) and (15) of RS method are equivalent to the combination of assumption (7) of DIH method.

3.3 Equivalence between RS and SPA Method

Proposition 3: When$n = 2$, the hypotheses (14) and (15) of RS method are equivalent to the combination hypothesis
$E\left\{\left\|\bigcup_{m=0}^{2^{b-1}-2}X_{2m+1}\right\|\right\}=E\left\{\left\|\bigcup_{m=0}^{2^{b-1}-2}Y_{2m+1}\right\|\right\}$ of SPA method.

Prove:

In section 3.1, the hypothesis (7) of DIH method is equivalent to the hypothesis (11) of SPA method. And in section 3.2, when $n = 2$, $m = 0, \cdots, 2^{b-1} - 2$, the assumptions (14) and (15) of RS method are equivalent to the combination of assumption (7) of DIH method. Hence, when $n = 2$, the assumptions (14) and (15) of RS method are equivalent to the combination hypothesis $E\left\{\left\|\bigcup_{m=0}^{2^{b-1}-2} X_{2m+1}\right\|\right\} = E\left\{\left\|\bigcup_{m=0}^{2^{b-1}-2} Y_{2m+1}\right\|\right\}$ of SPA method.

From 3.1, 3.2 and 3.3, it can be found that all of three methods depend on the weak correlation between the LSB plane and the remained bit planes though the different implementation methods. This weak correlation decreases with the increase of the embedded message and is represented as the assumption (12). From this section, the assumptions (7) and $\sum_{m=i}^{j} a_{2m,2m+1}g_{2m} = \sum_{m=i}^{j} a_{2m+2,2m+1}g_{2m+2}$ in DIH method are equivalent to (11) and (12) in SPA method; when $n = 2$, the assumptions (14) and (15) based on RS method equal to the special example of (12), viz. $\left\|\bigcup_{m=0}^{2^{b-1}-2} A_{2m+1}\right\| = \left\|\bigcup_{m=0}^{2^{b-1}-2} B_{2m+1}\right\|$. Consequently, it is concluded that DIH, SPA and RS methods are based on the same kind of hypothesis and are virtually similar.

4 Conclusions

Image steganalysis has attracted the increasing attention recently, and the LSB steganalysis is one of the most active research topics. SPA, RS and DIH are three powerful LSB steganalysis methods. In this paper, we make a comparison analysis among SPA, RS and DIH method, and present an equivalence proving of them. The proving process includes three parts, and three propositions are respectively proofed in these sections. This equivalence proving offers a theory base for the study of an approach that can synchronously resist these three kinds of steganalysis methods, which we will aim at.

References

1. A. Westfeld, "Detecting low embedding rates", Proceedings of the 5th Information Hiding Workshop, Volume 2578 of Springer LNCS, 2003, 324–339.
2. Sorina Dumitrescu, Xiaolin Wu, and Zhe Wang, "Detection of LSB Steganography via Sample Pair Analysis", IEEE Transactions on Signal Processing, VOL.51, NO.7, 2003, 1995–2007.
3. S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis", Proceedings of the 5th Information Hiding Workshop, Volume 2578 of Springer LNCS, 2003, 355–372.
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. Volume 4675 of SPIE, 2002, 1-13.

5. J. Fridrich, M. Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," Proceedings of ACM Workshop Multimedia Security, Ottawa, ON, Canada, Oct.5, 2001, 27-30.
6. T. Zhang; X. Ping. "Reliable detection of LSB steganography based on the difference image histogram", Proceedings of IEEE ICASSP 2003, Volume 3: 545-548.
7. T. Zhang, X. Ping. "A new approach to reliable detection of LSB steganography in natural images", Signal Processing, Elsevier, Volume 83 ,Issue 10, 2003, 2085-2093.
8. P. Lu, X. Luo et. al. "An Improved Sample Pairs Method for Detection of LSB Embedding", Proceedings of the 6th Information Hiding Workshop, Volume 3200 of Springer LNCS, 2004, 116-128.
9. X. Luo, B. Liu, F. Liu, "Improved RS Method for Detection of LSB Steganography", Proceedings of International Conference on Computational Sciences & Its Applications (ICCSA 2005), Volume 3481 of Springer LNCS, 2005, 508-516.
10. Andrew D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE Signal Processing Letters, vol. 12, No. 6, June, 2005, 441-444.
11. T. Zhang, X. Ping. "Reliable Detection of Spatial LSB Stegan0graphy Based on Difference Histogram", Journal of Software, 2004, l5(1)l5l~l58. (Chinese).

Appendix

If $(s_k, \tilde{s}_k)$ belongs to $R(-M)$, then s_k and $\tilde{s}_k$ are equivalent, or the larger s_k becomes smaller or the smaller s_k becomes larger through applying F_1 into s_k. Namely, $(s_k, \tilde{s}_k)$ may be under one of the following three cases:

$$\begin{cases} s_k > \tilde{s}_k, \text{ if } s_k \bmod 2 \ = 1 \\ s_k < \tilde{s}_k, \text{ if } s_k \bmod 2 \ = 0 \\ s_k = \tilde{s}_k \end{cases},$$

Then,s_k belongs to

$$\left(\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} H_{11,2m}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} H_{00,-2m}\right).$$

Replacing m by $m+1$ in $\left(\bigcup_{m=0}^{2^{b-1}-1} H_{11,2m}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} H_{00,-2m}\right)$ of the above formula, the below formula can be obtained:

$$\left(\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right) \cup \left(\bigcup_{m=-1}^{2^{b-1}-2} H_{11,2m+2}\right) \cup \left(\bigcup_{m=-1}^{2^{b-1}-2} H_{00,-2m-2}\right),$$

viz.

$$\left(\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right) \cup H_{00,0} \cup H_{11,0} \cup \left(\bigcup_{m=0}^{2^{b-1}-2} H_{11,2m+2}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-2} H_{00,-2m-2}\right). \tag{28}$$

If s_k belongs to $\left(\bigcup_{m=0}^{2^{b-1}-1} B_{2m+1}\right) \cup \left(\bigcup_{m=0}^{2^{b-1}-1} B_{-2m-1}\right) \cup H_{00,0} \cup H_{11,0}$, then its adjacent pixel $\tilde{s}_k$ must also be one element of

$\left(\overset{2^{b-1}-1}{\underset{m=0}{\cup}} B_{2m+1}\right) \cup \left(\overset{2^{b-1}-1}{\underset{m=0}{\cup}} B_{-2m-1}\right) \cup H_{00,0} \cup H_{11,0}$ and the pixel pair $(s_k, \tilde{s}_k)$ must be the element of $R(-M)$. If s_k belongs to $\left(\overset{2^{b-1}-2}{\underset{m=0}{\cup}} H_{11,2m+2}\right) \cup \left(\overset{2^{b-1}-2}{\underset{m=0}{\cup}} H_{00,-2m-2}\right)$, then $(s_k, \tilde{s}_k)$ must belong to $R(-M)$, but $\tilde{s}_k$ must not be the element of $\left(\overset{2^{b-1}-2}{\underset{m=0}{\cup}} H_{11,2m+2}\right) \cup \left(\overset{2^{b-1}-2}{\underset{m=0}{\cup}} H_{00,-2m-2}\right)$. Therefore, we can obtain the equation (20),

$$\begin{aligned}\|R(-M)\| = \tfrac{1}{2}\Bigg(&\left\|\overset{2^{b-1}-1}{\underset{m=0}{\cup}} B_{2m+1}\right\| + \left\|\overset{2^{b-1}-1}{\underset{m=0}{\cup}} B_{-2m-1}\right\| + \|H_{00,0}\| + \|H_{11,0}\|\Bigg) \\ &+ \left\|\overset{2^{b-1}-1}{\underset{m=1}{\cup}} H_{11,2m}\right\| + \left\|\overset{2^{b-1}-1}{\underset{m=1}{\cup}} H_{00,2m}\right\|.\end{aligned}$$