SCIENCE CHINA
Information Sciences

• RESEARCH PAPERS •

December 2010 Vol. 53 No. 12: 2472–2484
doi: 10.1007/s11432-010-4105-7

Modification ratio estimation for a category of adaptive steganography

LUO XiangYang[1], LIU FenLin[1], YANG ChunFang[1]* & LIAN ShiGuo[2]

[1]*Zhengzhou Information Science and Technology Institute, Zhengzhou* 450002, *China;*
[2]*France Telecom R&D Beijing, Beijing* 100080, *China*

Received April 12, 2010; accepted August 9, 2010

Abstract This paper investigates the detection of adaptive image steganography. Firstly, the sample pair analysis model of multiple least-significant bits (MLSB) replacement is analyzed, and the conditions under which the adaptive steganography can be detected via this model are given. For the category of adaptive steganography satisfying these conditions, a general quantitative steganalysis method is presented based on specific areas and sample pair analysis. Then, for a typical adaptive steganography, some concrete methods are proposed to select specific areas and trace sets of sample pairs, and estimate the stego modification ratios. Experimental results show that the proposed methods can estimate the stego modification ratio accurately. This verifies the validity of the proposed general quantitative steganalysis method.

Keywords adaptive steganography, steganalysis, MLSB (multiple least significant bits), sample pair analysis, modification ratio

Citation Luo X Y, Liu F L, Yang C F, et al. Modification ratio estimation for a category of adaptive steganography. Sci China Inf Sci, 2010, 53: 2472–2484, doi: 10.1007/s11432-010-4105-7

1 Introduction

Steganography is the art of covert communication. Along with steganography, the opposite, steganalysis, is also one of the key technologies of multimedia information security [1, 2]. With the development of steganalysis technique, the steganography method based on simple least significant bit (LSB) replacement becomes no longer secure. There exist many methods which can not only detect LSB replacement steganography reliably, but also estimate the embedding ratio, such as χ^2 method [3], RS (regular and singular groups) method [4], SPA (sample pair analysis) method [5], WS (weighted stego-image) method [6] and some improved variants [7, 8] of them. In order to resist the above steganalysis methods and meet the requirements of covert communication, some steganography methods with higher security and large capacity have been proposed, such as LSB matching steganography, stochastic modulation steganography and adaptive steganography.

For LSB matching and stochastic modulation steganography, there have been some quantitative steganalysis methods available [9, 10] which can estimate the stego message ratio or modification ratio [11]. For adaptive steganography, the bit plane complexity segmentation (BPCS) steganography is a typical one, which is firstly proposed by Kawaguchi et al. [12]. The BPCS steganography partitions the image

*Corresponding author (email: chunfangyang@126.com)

into blocks with fixed size. Then, if the texture complexity of a Gray code bit plane of a block is larger than a given threshold, bits in this Gray code bit plane will be replaced by the secret message. This kind of steganography can be implemented easily and achieve high imperceptibility and capacity. Moreover, they can also be extended from spatial domain to transformed domain or temporal domain medias, such as JPEG2000 images or compressed videos [13, 14]. After this, some new adaptive steganography methods [15, 16] have been proposed. For example, to resist the attacks of RS, SPA and some other typical LSB steganalysis methods, Nguyen et al. [15] presented an adaptive multiple bit planes image steganography (MBPIS) method. This method is an important improvement of BPCS steganography. It adopts a bit plane complexity measurement which depends on the higher bit planes, and embeds the message from higher bit planes to lower bit planes. And thus, the later embedding will not affect the complexity measurement values of the higher and current bit planes. Additionally, this method utilizes the matrix encoding technique to reduce the modifications caused by embedding, which makes the stego images hard to be detected. Because the adaptive steganography is highly imperceptible and difficult to be detected, the research on corresponding steganalysis owns high theoretical and practical value.

The adaptive steganography can be detected by some blind steganalysis methods, such as the blind steganalysis methods proposed by Wang et al. in [17] and by us in [18]. However, blind steganalysis method can just distinguish the stego images, but cannot estimate the embedding ratio or modification ratio. In literatures, the steganalysis methods designed specifically for adaptive steganography are sparse. Currently, several existing steganalysis methods for adaptive steganography mainly focus on BPCS steganography. For example, Kim et al. [19] took the lead in detecting the spatial domain BPCS steganography proposed in [12] by the χ^2 test method. Then, Niimi et al. [20] pointed out that the complexity histogram of the stego image generated by BPCS steganography in [12] would appear significantly discontinuous in the positions of threshold and one minus threshold. Considering this defect, Zhang et al. [21] defined a measure to scale the discontinuity of complexity histogram which can be used to detect the BPCS steganography in [12] automatically. Since BPCS steganography destroys the isotropy of spatial domain cover and the Gaussian-like characteristic of transformation domain cover's coefficient histogram, Yu et al. [22] used the χ^2 test to determine whether the given image satisfies these characteristics in order to detect the spatial domain or transformation domain BPCS steganography. Julio et al. [23] replaced the artificial neural network with support vector machine to solve the problem that the blind steganalysis in [24] cannot detect BPCS stego images effectively. However, for the MBPIS steganography proposed in [15] to resist the RS method, there is just a steganalysis method proposed in [25] by adapting the RS method to non-flat areas. In a word, some methods are available for detecting BPCS and MBPIS steganography. But, the quantitative steganalysis methods still have not appeared in literatures.

In some adaptive steganography methods, for the areas whose complexities are larger than the threshold, the secret message is embedded not only into the LSB plane, but also into the higher bit planes. Currently, some steganalysis methods have been proposed to estimate the embedding ratios in higher bit planes. For example, Yu et al. [26] extended the WS method to estimate the embedding ratio of a typical multiple least significant bits (MLSB) replacement steganography pattern. Ker [27] and we [28] independently extended the sample pair analysis method designed for LSB replacement, and presented the I2Couples, 2Couples and QEM method to estimate the embedding ratio of 2LSB replacement steganography. Yu et al. [29] presented methods to estimate the embedding ratios of two typical MLSB replacement steganography patterns based on sample pair analysis. In [30], we presented a sample pair analysis model for MLSB replacement steganography, then based on this model, gave two steganalysis methods to estimate the embedding ratios of two typical MLSB replacement patterns. After this, we improved the method in [30] to make it able to estimate the embedding ratio in each bit plane. The improved method was called IDMSPA method [31], and would be called ID3SPA method when being used to estimate the embedding ratios in the three least significant bit planes.

This paper analyzes the problems faced by existing methods when they are used to detect the adaptive steganography. Then, the research results on steganalysis of MLSB replacement are applied to the detection of adaptive steganography. And the conditions under which the adaptive steganography can be detected via the sample pair analysis model of multiple bit-planes replacement are given. For the category of adaptive steganography satisfying these conditions, a general quantitative steganalysis method is presented based on the stego areas treated equivalently and the sample pair analysis. Then, for a typical adaptive steganography, the concrete methods are proposed to select the stego areas, trace sets of stego sample pairs, and estimate the stego modification ratios. Experimental results show that the proposed method can estimate the stego modification ratio accurately. This verifies the validity of the proposed general quantitative steganalysis method.

2 The problems

Most of existing quantitative steganalysis methods focus on sequence or random embedding. Thus, when estimating the modification ratio or embedding ratio, it is usual to think that there is no correlation between the embedded messages and pixels. But, the adaptive steganography usually does not embed message or just embeds few messages into the smooth areas, while embedding more messages into the textured areas. The adaptive steganography considers the difference among different areas, embeds messages into different areas with different ratios, and then introduces the correlation between the embedded messages and the cover. This kind of correlation breaks down the assumption based on by existing quantitative steganalysis methods, and invalidates these methods. The idea to solve this problem is to search for the stego areas treated equivalently, such as textured areas. In these areas, the embedded messages and pixels of cover image can be thought of as mutually independent.

The existing quantitative steganalysis methods usually utilize the fixed relationships among some statistics which are obtained from the whole image, viz. the statistical characteristics of the image. Even if the steganalyzers can identify the stego areas treated equivalently, the statistics obtained from these areas may not satisfy the statistical characteristics of the whole image. This is also a key problem when applying existing quantitative steganalysis methods to the adaptive steganography methods. For this problem, we need to search for the statistical characteristics which are utilized by existing methods and are still satisfied in the stego areas treated equivalently.

Therefore, when applying the existing quantitative steganalysis methods to the adaptive steganography methods, the following two problems should be solved:

1) How to search for the stego areas treated equivalently when embedding?

2) How to search for the statistical characteristics which are utilized by existing methods and are still satisfied in the stego areas treated equivalently?

From the above point of view, we will first introduce the sample pair analysis model of MLSB replacement which is called MSPA model, and then analyze the conditions under which the adaptive steganography methods can be analyzed by MSPA model.

3 Sample pair analysis model of MLSB replacement

The digital image is represented by the succession of samples $s_1, s_2, \ldots, s_N$, $0 \leqslant s_i \leqslant 2^b - 1$, where N denotes the total number of pixels in an image and b denotes the total number of bits in a pixel. A two-tuple $\langle i,j\rangle$ is named a pixel pair, where i and j are the indexes of pixels and $1 \leqslant i, j \leqslant N$. Let $\Re$ be the set of all adjacent pixel pairs $\langle i,j\rangle$, $i \neq j$. In [30], a trace set C_m of $\Re$ was defined as follows:

$$C_m = \{\langle i,j\rangle \,|\, |\lfloor s_i/L\rfloor - \lfloor s_j/L\rfloor| = m, i \neq j\}, \tag{1}$$

where $L = 2^l$, $0 \leqslant m \leqslant \tilde{L} - 1$, $\tilde{L} = 2^{b-l}$, and l denotes that the l least significant bit planes of the image are modified when embedding. The trace set C_m $(0 \leqslant m \leqslant \tilde{L} - 1)$ can be partitioned into L^2 trace subsets as follows:

$$Q_{0,\tau_1,\tau_2} = \{\langle i,j\rangle | s_i = Lk + \tau_1, s_j = Lk + \tau_2, 0 \leqslant k \leqslant \tilde{L} - 1, 1 \leqslant i \neq j \leqslant N\}, m = 0, \tag{2}$$

$$Q_{m,\tau_1,\tau_2} = \left\{ \langle i,j\rangle \,\middle|\, \begin{array}{l} s_i = L(k-m) + \tau_1, s_j = Lk + \tau_2, \text{ or } s_i = Lk + L - 1 - \tau_1, \\ s_j = L(k-m) + L - 1 - \tau_2, m \leqslant k \leqslant \tilde{L} - 1, 1 \leqslant i \neq j \leqslant N, \end{array} \right\} 1 \leqslant m \leqslant \tilde{L} - 1, \tag{3}$$

where $0 \leqslant \tau_1,\ \tau_2 \leqslant L-1$.

Because the MLSB replacement modifies only the l least significant bit planes of the images, each pixel pair will be modified by L^2 possible patterns which are defined as so-called L^2 modification patterns $[\pi_1, \pi_2]$, $0 \leqslant \pi_1, \pi_2 \leqslant L-1$. Thus, if a pixel pair $\langle i, j\rangle$ belongs to the trace subset Q_{m,τ_1,τ_2} and is modified by pattern $[\pi_1, \pi_2]$ during MLSB replacement, then after being modified, the two pixels' MLSBs of this pixel pair can be obtained by carrying out exclusive OR between the elements in modification pattern and the pixels' MLSBs of the cover pixel pair. According to the definitions of trace subsets in (2) and (3), the stego pixel pair must belong to trace subset $Q'_{m,\tau_1\oplus\pi_1,\tau_2\oplus\pi_2}$, where $\oplus$ denotes the exclusive OR operation. For convenience, each pixel is denoted by s_i or s'_i depending on whether the pixel is obtained from the natural or stego image of MLSB steganography. The same convention is also applied to the set such that Z and Z' are the sets before and after MLSB steganography respectively.

According to the l LSBs of the larger pixel of a pixel pair, $\Re$ can also be partitioned into the following new subsets:

$$X_{Lm+u} = \{\langle i,\ j\rangle \| s_i - s_j| = Lm + u,\ \max(s_i, s_j) \bmod L < u,\ 1 \leqslant i \neq j \leqslant n\}, \tag{4}$$

$$Y_{Lm+u} = \{\langle i,\ j\rangle \| s_i - s_j| = Lm + u,\ \max(s_i, s_j) \bmod L \geqslant u,\ 1 \leqslant i \neq j \leqslant n\}, \tag{5}$$

where $0 \leqslant m \leqslant \tilde{L}-1$, $0 \leqslant u \leqslant L-1$, $\max(s_i, s_j)$ is to get the larger one from s_i and s_j. Then for the natural images, because it is about equally probable that the l LSBs of the larger component of a pixel pair differing by $Lm+u$ is $0, 1, \ldots, L-2$ or $L-1$, the following formula can be obtained:

$$u|Y_{Lm+u}| \approx (L-u)|X_{Lm+u}|, \tag{6}$$

where $|\cdot|$ denotes the cardinality of set $\cdot$. Additionally, the relationships between X_{Lm+u}, Y_{Lm+u} and $Q_{m,\pi_1,\ \pi_2}$ were given in [30], for $0 \leqslant u \leqslant L-1$, as follows:

$$X_{Lm+u} = \bigcup_{v=0}^{u-1} Q_{m+1,L+v-u,v},\ 0 \leqslant m \leqslant \tilde{L}-2, \tag{7}$$

$$Y_{Lm+u} = \bigcup_{v=u}^{L-1} Q_{m,v-u,v}, 1 \leqslant m \leqslant \tilde{L}-1, \tag{8}$$

$$Y_u = \bigcup_{v=u}^{L-1} (Q_{0,v-u,\,v} \cup Q_{0,v,\,v-u}). \tag{9}$$

4 General quantitative steganalysis of adaptive steganography based on specific areas and MSPA model

According to the definition of trace sets in the MSPA model, the trace set which a pixel pair belongs to is determined by the absolute difference between the high $(b-l)$ bits of the two adjacent pixels in this pixel pair. If the absolute difference between the high $(b-l)$ bits of two pixels s_i and s_j is m, then

$$Lm - L + 1 \leqslant |s_i - s_j| \leqslant Lm + L - 1. \tag{10}$$

This indicates that if the complexity of an image area is determined by the difference between two pixels, the complexity of this area is reflected in a certain extent by the trace sets which the pixel pairs in this area belong to. When m is large, the pixel pairs contained by the trace set C_m in the MSPA model possibly all belong to certain textured areas treated equivalently. Thus, the MSPA model can possibly be used to analyze some adaptive steganography.

The MSPA model assumes that the steganography modifies just the l least significant bits of pixels, and each pixel pair transits among the trace subsets of the trace set containing the pixel pair.

Additionally, from the analysis in section 2, we can see that when applying the existing quantitative steganalysis methods to the adaptive steganography methods, it is necessary to search for the stego areas treated equivalently for message embedding, and in these areas, search for the statistical characteristics on which the existing methods depend.

The existing quantitative steganalysis methods based on the MSPA model usually assume that the message is spread in all pixels, viz. each pixel is treated equivalently. But, when the message is embedded by the adaptive steganography, if the pixel pairs in a trace set belong to areas treated differently, then bits in the same positions of these pixels will be modified with different possibilities. This would increase the difficulty in analyzing the transition possibilities among trace subsets because it is no longer suitable for the condition that the bits in the same bit plane would be modified with the equal possibilities. However, if the trace sets contain only pixel pairs which belong to the stego areas treated equivalently, the statistical characteristics of these trace sets based on by the existing methods are still satisfied. Thus, the trace sets used for quantitative steganalysis of adaptive steganography must just contain pixels in the stego areas treated equivalently. We call these trace sets the stego trace sets treated equivalently.

On the basis of above analysis, the following proposition gives the conditions under which the adaptive steganography methods can generate the stego trace sets treated equivalently.

Proposition. For the adaptive steganography method which embeds message into the areas whose complexity is larger than a fixed threshold T, if there is a function F so that for arbitrary two adjacent pixels s_i and s_j in the same area, $f(A_k) \geqslant F(m)$, where A_k is the area containing s_i and s_j, $f(A_k)$ is the measure of the complexity of the area A_k, and m is the absolute difference between the high $(b-l)$ bits of s_i and s_j, then when $F(m) > T$, the area A_k is the stego area treated equivalently, and the trace set C_m contains just pixels in the stego areas treated equivalently.

Proof. For arbitrary two adjacent pixels s_i and s_j in the same area, based on the function F, $f(A_k) \geqslant F(m)$, when $F(m) > T$, that is, $f(A_k) \geqslant F(m) > T$. And because the adaptive steganography method embeds message into the areas whose complexity is larger than a fixed threshold T, certainly, the area containing s_i and s_j is the stego area treated equivalently.

For arbitrary adjacent pixel pair $\langle \alpha, \beta \rangle$ in C_m, we have $|\lfloor s_\alpha/L \rfloor - \lfloor s_\beta/L \rfloor| = m$. From the conditions in the proposition, it can be seen that the function F leads to the complexity $f(A_\gamma)$ of the area A_γ containing s_α and s_β satisfying $f(A_\gamma) \geqslant F(m)$. And because $F(m) > T$, we have $f(A_\gamma) \geqslant F(m) > T$. Therefore, when embedding via this adaptive steganography method, the pixels in the area A_γ will be treated equivalently and the messages can be embedded randomly. Consequently, when $F(m) > T$, the trace set C_m contains just pixels in the stego areas treated equivalently.

Thus, the proof of this proposition is completed.

The above analysis shows that the adaptive steganography method which can be analyzed via MSPA model must not only modify just the l least significant bits, but also adopt the complexity measure and threshold set which satisfy the above proposition. For this category of adaptive steganography methods, the bits in the same positions of pixels in the stego trace sets treated equivalently would be modified with the equal probabilities. And these trace sets can be utilized to design the quantitative steganalysis methods based on the MSPA model.

The main steps of the general quantitative steganalysis of the adaptive steganography based on specific areas and MSPA model are as follows:

I. According to the complexity measure adopted by the given adaptive steganography, construct the function F which makes $f(A_k) \geqslant F(m)$ and $F(m) > T$, where m is the absolute difference between the high $(b-l)$ bits of the adjacent pixels in the area A_k. Then, based on the constructed function F, search for the stego trace sets treated equivalently by the next step. If the function satisfying above conditions cannot be constructed, quit detecting.

II. From the formula $F(m) > T$, determine the stego trace sets treated equivalently.

III. For the determined stego trace sets treated equivalently, calculate the cardinalities of their trace subsets.

IV. Based on the cardinalities of the trace subsets of the stego trace sets treated equivalently, carry out the quantitative steganalysis of the given adaptive steganography method.

In the following content, two examples are given to introduce how to construct the function F, and then how to search for the stego trace sets treated equivalently.

1) The complexity measure of the area A_k is the maximum of the absolute differences between two pixels in this area, viz.

$$f(A_k) = \max(|s_i - s_j|, i, j \in A_k). \tag{11}$$

Obviously, $f(A_k) = \max(|s_i - s_j|, i, j \in A_k) \geqslant |s_i - s_j|$. Construct

$$F(m) = Lm - L + 1. \tag{12}$$

Then, from (10), we can obtain $f(A_k) \geqslant |s_i - s_j| \geqslant Lm - L + 1 = F(m)$. Thus, if the absolute difference m between the high $(b - l)$ bits of s_i and s_j satisfies $F(m) = Lm - L + 1 > T$, viz. $m > (T + L - 1)/L$, the corresponding trace set C_m is the stego trace set treated equivalently.

2) The complexity measure of the area A_k is the average over the absolute differences between two pixels in this area, viz.

$$f(A_k) = \sum_{i,j \in A_k} |s_i - s_j|/n, \tag{13}$$

where n denotes the number of pixel pairs in the area A_k. It can be seen that $f(A_k) = \sum_{i,j \in A_k} |s_i - s_j|/n \geqslant |s_i - s_j|/n$. Construct

$$F(m) = (Lm - L + 1)/n, \tag{14}$$

then, from (10), it follows that $f(A_k) \geqslant |s_i - s_j|/n \geqslant (Lm - L + 1)/n = F(m)$. Thus, if the absolute difference m between the high $(b - l)$ bits of s_i and s_j satisfies $F(m) = (Lm - L + 1)/n > T$, viz. $m > (nT + L - 1)/L$, the corresponding trace set C_m is the stego trace set treated equivalently.

In section 5, for the typical adaptive steganography method MBPIS in [15], the corresponding quantitative steganalysis method is designed based on the above idea.

5 Quantitative steganalysis of adaptive steganography MBPIS

5.1 Brief introduction to adaptive steganography MBPIS

In [15], the adaptive multiple bit planes image steganography (MBPIS) method was presented. This method converts a pixel value in natural binary code into another value in Gray code as follows:

$$\begin{cases} g_b = d_b, \\ g_i = d_i \oplus d_{i+1}, \quad 1 \leqslant i \leqslant b - 1, \end{cases} \tag{15}$$

where d_i and g_i denote the ith bits of the pixel value d in natural binary code and the pixel value g in Gray code respectively, and the first bit is LSB. Then, the converted image is decomposed into b Gray code bit planes, $G_b G_{b-1} G_{b-2} \ldots G_i \ldots G_1$. The process of converting the pixel value in Gray code into the pixel value in natural binary code is defined as

$$\begin{cases} d_b = g_b, \\ d_i = g_i \oplus d_{i+1}, \quad 1 \leqslant i \leqslant b - 1. \end{cases} \tag{16}$$

The MBPIS method does not embed data into the smooth area, but embeds data into the textured area adaptively. In [15], the smooth area of a bit plane is called the flat area, and the textured area is called the non-flat area. To identify the flat areas, the image is partitioned into non-overlapping blocks with size of $n_1 \times n_2$ (n_1 and n_2 are less than the width and height of the image respectively, and their values are usually 2, 3 and 4.). The complexity measure of each block's ith Gray code bit plane depends on the differences between two contained pixels' higher bits in Gray code as follows:

$$f(A_k, i) = \max\{|\lfloor p_1/2^i \rfloor - \lfloor p_2/2^i \rfloor|, |\lfloor p_1/2^i \rfloor - \lfloor p_3/2^i \rfloor|, \ldots, |\lfloor p_1/2^i \rfloor - \lfloor p_{n_1 n_2}/2^i \rfloor|\}, \tag{17}$$

where A_k denotes the kth block of the cover image, p_j denotes the Gray code value of the jth pixel in the block and p_1 denotes the Gray code value of the pixel in the upper left corner of the block. If $f(A_k, i)$

is not larger than the given threshold t, viz. $f(A_k, i) \leqslant t$, the ith Gray code bit plane of the block A_k is flat. Otherwise, it is non-flat. The threshold adopted in [15] is 0 or 1.

The MBPIS method determines the number l $(1 \leqslant l < b)$ of Gray code bit planes used to embed message first. Then, some secret message is embedded into the Gray code bit planes, G_l, G_{l-1}, $\ldots$, G_1, in turn. When embedding the secret message into the ith Gray code bit plane G_i $(1 \leqslant i \leqslant l)$, the method searches for the non-flat blocks first, and then embeds the secret message into the ith Gray code bit plane of the non-flat blocks randomly. Finally, the image in Gray code is converted into the image in natural binary code. For the 8-bit grayscale images, embedding message into the fifth or higher bit plane will cause significant vision distortion. Therefore, the number of bit planes used in MBPIS method should be no larger than 4. In order to improve the security of steganography, the MBPIS method utilizes matrix encoding technique to reduce the number of modification. When extracting the message, the receiver just needs to extract the bits in non-flat areas from the lth to first Gray code bit plane in turn and decode the bits into secret message by the shared key.

The embedding procedure of the MBPIS method shows that for the fixed number l of stego bit planes, the MBPIS method modifies just the l least significant Gray code bit planes. Then, from the process of converting images in Gray code into images in natural binary code in (16), it can be derived that the MBPIS method also modifies just the l least significant natural binary bit planes. Therefore, in the following subsection, we try to apply the MSPA model to the quantitative steganalysis of the MBPIS method on the basis of the idea given in section 4.

5.2 Selecting the non-flat areas treated equivalently

The MBPIS method calculates the complexity measures of each block's Gray code bit planes by (17). For the threshold t, denote the set of blocks which are non-flat in the ith Gray code bit plane by

$$\mathbf{NF}_{i,t} = \{A_k | f(A_k,\ i) > t\}. \tag{18}$$

And the pixels in the blocks belonging to $\mathbf{NF}_{i,t}$ are given by

$$\mathbf{Nf}_{i,t} = \{s_j | f(A_k,\ i) > t,\ s_j \in A_k\}. \tag{19}$$

If the blocks which are non-flat in the higher bit planes are sometimes flat and sometimes non-flat in the lower bit planes, the areas composed of these blocks are not the areas treated equivalently. Then, the problem whether the pixels which are non-flat in the higher bit planes are also flat in the lower bit planes will be answered by the following theorem.

Theorem. The pixels which are non-flat in the higher bit plane are also non-flat in the lower bit planes.

Proof. When a pixel is non-flat in the ith bit plane, there must exist a pixel s_j belonging to the same block so that the absolute difference $\bar{t}$ between the high $(b-i)$ bits of it and the pixel s_j^* in the upper left corner of the same block is larger than t, viz. $\bar{t} = |\lfloor s_j^*/2^i \rfloor - \lfloor s_j/2^i \rfloor| > t$. Then, the absolute difference between the high $(b-i+1)$ bits of these two pixels is

$$\begin{aligned} |\lfloor s_j^*/2^{i-1} \rfloor - \lfloor s_j/2^{i-1} \rfloor| &= |\lfloor s_j^*/2^i \rfloor \times 2 + s_{j,i}^* - \lfloor s_j/2^i \rfloor \times 2 - s_{j,i}| \\ &= |(\lfloor s_j^*/2^i \rfloor - \lfloor s_j/2^i \rfloor) \times 2 + s_{j,i}^* - s_{j,i}| \\ &= |2\bar{t} + s_{j,i}^* - s_{j,i}|, \end{aligned}$$

where $s_{j,i}^*$ and $s_{j,i}$ are the ith bits of s_j^* and s_j respectively. $\bar{t} \geqslant 1$ can be obtained from $t \geqslant 0$. So

$$|\lfloor s_j^*/2^{i-1} \rfloor - \lfloor s_j/2^{i-1} \rfloor| \geqslant 2\bar{t} - 1 \geqslant \bar{t} > t.$$

Therefore, the $(i-1)$th bit plane of the block is also non-flat and the pixels in this block are also non-flat in the $(i-1)$th bit plane.

Consequently, the proof of this theorem is completed.

Accordingly, when $r < i$,

$$\mathbf{Nf}_{r,t} \supseteq \mathbf{Nf}_{i,t}. \tag{20}$$

If the MBPIS method modifies the rth natural binary bits of the pixels in $\mathbf{Nf}_{r,t}(1 \leqslant r < l)$ with ratio p_r, then because $\mathbf{Nf}_{r,t} \supseteq \mathbf{Nf}_{l,t}$, the rth natural binary bits of the pixels in $\mathbf{Nf}_{l,t}$ would also be modified with ratio p_r. Therefore, the areas composed of the pixels which are non-flat in the higher bit planes are also the non-flat area treated equivalently. So far, the first problem pointed out in section 2 has been solved.

5.3 Selecting the stego trace sets treated equivalently

In section 4, we have pointed out that for the given adaptive steganography, it is necessary to search for the stego trace sets C_m treated equivalently. The pixel pairs in these trace sets should belong to the stego areas treated equivalently whose l least significant bit planes are non-flat. This can ensure that there are the transition relationships among their trace subsets introduced in section 3 and bits in the same positions of their pixels will be modified with equivalent probabilities.

In order to ensure that the two pixels in a pixel pair do not belong to two different areas, assume that the size of the block $n_1 \times n_2$ is known, and just calculate the pixel pairs in each block. But, if the absolute difference M between the high $(b-l)$ bits of the two pixels' Gray code values in a adjacent pixel pair is larger than t, this pixel pair does not always belong to the non-flat areas. This is because neither of the two pixels in this pixel pair is in the upper left corner of the block possibly. However, the complexity measure of the lth Gray code bit plane of the block A_k containing them must satisfies

$$f(A_k, l) \geqslant M/2. \tag{21}$$

Thus, if the absolute difference M between the high $(b-l)$ bits of the two adjacent pixels' Gray code values satisfies $M > 2t$, the lth Gray code bit plane of the block containing them is non-flat.

In the MSPA model, the trace set is determined by the absolute difference between the high $(b-l)$ bits of two pixels' natural binary values. But in the MBPIS method, the complexity is measured by the absolute difference between the high $(b-l)$ bits of two pixels' Gray code values. Thus, firstly, it is necessary to establish the mapping relationships between the absolute differences in natural binary code and in Gray code, viz. to know the possible absolute differences in Gray code of two natural binary values with the given absolute difference m. Table 1 shows the possible absolute difference between the high $(b-l)$ bits of two pixels' natural binary values when the absolute difference between the high $(b-l)$ bits of their Gray code values is 0–15. In the MBPIS method, the threshold used to select the non-flat areas is usually 0 or 1, and there are few pixel pairs with the absolute difference between the high $(b-l)$ bits of their Gray code values being larger than 15. Thus, Table 1 only supplies the cases the absolute differences are 0, 1, …, 15.

Let the function $M = Map(m)$ denote the mapping from the absolute difference in natural binary to the absolute difference in Gray code in Table 1. We can construct the function

$$F(m) = Map(m)/2,$$

and then, from (21), we obtain $f(A_k, l) \geqslant M/2 = Map(m)/2 = F(m)$.

When $t = 0$, as seen from Table 1, if the absolute difference m between the high $(b-l)$ bits of two pixels in natural binary code satisfies $m \geqslant 1$, m must satisfy $F(m) = Map(m)/2 > 0$. So, by the proposition in section 4, the corresponding trace sets for $m \geqslant 1$ are the stego trace sets treated equivalently.

When $t = 1$, as seen from Table 1, if the absolute difference between the high $(b-l)$ bits of two pixels in natural binary are 6, 7, 8, 12, 13, 14, …, 19, 22, 23, …, 31, m must satisfy $F(m) = Map(m)/2 > 1$. So, from the proposition in Section 4, the corresponding trace sets for m=6, 7, 8, 12, 13, 14, …, 19, 22, 23, …, 31 are the stego trace sets treated equivalently.

In the MBPIS method, the threshold used to select the non-flat areas is usually 0 or 1, so the examples are just supplied for these two cases.

5.4 Estimating the modification ratio of MBPIS

If the MBPIS method modifies the kth bits of the pixels' natural binary values in $\mathbf{Nf}_{k,t}(1 \leqslant k < l)$ with ratio p_k, then because $\mathbf{Nf}_{k,t} \supseteq \mathbf{Nf}_{l,t}$, the kth bits of the pixels' natural binary values in $\mathbf{Nf}_{l,t}$ must be

Table 1 Possible absolute differences m between the high $(b-l)$ bits of two pixels' natural binary values when the absolute difference between the high $(b-l)$ bits of their Gray code values is M

Absolute difference M in Gray code	Absolute difference m in natural binary code	Absolute difference M in Gray code	Absolute difference m in natural binary code
0	0	8	1, 3, 5, 7, 9, 11, 13, 15, 16, ...
1	1, 2, 5, 10, 21, ...	9	2, 5, 6, 10, 11, 14, 15, 17, 18, 26, ...
2	1, 3, 4, 9, 11, 20, ...	10	4, 5, 7, 12, 13, 15, 17, 19, 25, 27, ...
3	2, 3, 6, 7, 9, 10, 18, 19, 22, ...	11	3, 6, 7, 9, 10, 13, 14, 18, 23, 25, 26, ...
4	1, 3, 5, 7, 8, 17, 19, 21, 23, ...	12	8, 9, 11, 13, 15, 24, ...
5	2, 3, 6, 7, 9, 13, 14, 18, 19, 22, ...	13	3, 7, 9, 10, 13, 14, 19, 22, 23, 25, 29, ...
6	4, 5, 7, 12, 13, 15, 17, 19, 20, ...	14	4, 9, 11, 12, 20, 21, 23, 28, ...
7	2, 5, 6, 10, 11, 14, 15, 17, 18, 21, ...	15	2, 5, 6, 10, 11, 14, 18, 21, 22, 26, 27, 30, ...

modified with ratio p_k too. Sequentially, from the definition of modification pattern, the probability that the modification pattern $[\pi_1, \pi_2]$ occurs in the l LSBs of a pixel pair in $\mathbf{Nf}_{l,t}$ is

$$\rho_{2l}([\pi_1, \pi_2]) = \prod_{k=1}^{l} q_k^{2-bit(\pi_1,k)-bit(\pi_2,k)} p_k^{bit(\pi_1,k)+bit(\pi_2,k)}, \tag{22}$$

where $q_k = 1 - p_k$, $bit(\pi_i, k)(i = 1, 2)$ denotes the kth bit of π_i. Consequently, for the stego trace sets treated equivalently in subsection 5.3, based on the modification patterns that must occur when a pixel pair transfers from one trace subset to another, we have

$$\boldsymbol{Q}'_{m,l} = \boldsymbol{A}_l^{\otimes 2} \boldsymbol{Q}_{m,l}, \tag{23}$$

where $\boldsymbol{A}_l = \left(\begin{smallmatrix} q_l & p_l \\ p_l & q_l \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} q_{l-1} & p_{l-1} \\ p_{l-1} & q_{l-1} \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} q_1 & p_1 \\ p_1 & q_1 \end{smallmatrix}\right)$, $\otimes$ is the operation of Kronecker product, $\boldsymbol{A}_l^{\otimes 2}$ is the 2nd Kronecker power of matrix $\boldsymbol{A}_l$ and $\boldsymbol{Q}_{m,l} = (|Q_{m,0,0}|, |Q_{m,0,1}|, \ldots, |Q_{m,L-1,L-1}|)^{\mathrm{T}}$.

As with [31], when $p_k \neq 1/2 (1 \leqslant k \leqslant l)$, from (23), the cardinality of each trace subset of cover image can be given by the function with the cardinalities of the trace subsets of stego image as coefficients and the modification ratios as unknown parameters, viz.

$$\boldsymbol{Q}_{m,l} = (\boldsymbol{A}_l^{-1})^{\otimes 2} \boldsymbol{Q'}_{m,l}, \tag{24}$$

where $\boldsymbol{A}_l^{-1}$ is the inverse matrix of $\boldsymbol{A}_l$.

Applying (24) to (7)–(9) respectively, $|X_{Lm+u}|$ and $|Y_{Lm+u}|$ can also be denoted by the functions with the cardinalities of the trace subsets of stego image as coefficients and the modification ratios as unknown parameters. Then, applying them to (6), the modification ratio in each bit plane of the natural binary values can be estimated as follows:

$$\begin{aligned} &(L-u) \sum_{\tau_1=0}^{L-1} \sum_{\tau_2=0}^{L-1} \sum_{v=0}^{u-1} \left(\prod_{k=1}^{l} P(p_k, L+v-u, \tau_1, v, \tau_2) |Q'_{m+1,\tau_1,\tau_2}| \right) \\ &- u \sum_{\tau_1=0}^{L-1} \sum_{\tau_2=0}^{L-1} \sum_{v=u}^{L-1} \left(\prod_{k=1}^{l} P(p_k, v-u, \tau_1, v, \tau_2) |Q'_{m,\tau_1,\tau_2}| \right) = 0, \end{aligned} \tag{25}$$

and

$$\begin{aligned} &(L-u) \sum_{\tau_1=0}^{L-1} \sum_{\tau_2=0}^{L-1} \sum_{v=0}^{u-1} \left(\prod_{k=1}^{l} P(p_k, L+v-u, \tau_1, v, \tau_2) |Q'_{1,\tau_1,\tau_2}| \right) \\ &- u \sum_{\tau_1=0}^{L-1} \sum_{\tau_2=0}^{L-1} \sum_{v=u}^{L-1} \left(\left(\prod_{k=1}^{l} P(p_k, v-u, \tau_1, v, \tau_2) + \prod_{k=1}^{l} P(p_k, v, \tau_1, v-u, \tau_2) \right) |Q'_{0,\tau_1,\tau_2}| \right) = 0, \end{aligned} \tag{26}$$

where $P(p_k, \pi_1, \tau_1, \pi_2, \tau_2) = (1-p_k)^{2-bit(\pi_1 \oplus \tau_1, k)-bit(\pi_2 \oplus \tau_2, k)} (-p_k)^{bit(\pi_1 \oplus \tau_1, k)+bit(\pi_2 \oplus \tau_2, k)}$, $1 \leqslant k \leqslant l$, $1 \leqslant m \leqslant \tilde{L} - 2$ and $1 \leqslant u \leqslant L - 1$. When $u = 0$, both two sides of (6) are always equal to 0, so (6) is not useful for discrimination between cover and stego images at this time and is discarded.

Following [31], the different m and u are combined, viz. the corresponding estimation equations for different m and u are summated to obtain the final equations for estimating the modification ratios. And when right-shifting all the pixels of an image r bits (the rightmost bit of a pixel value is its LSB), the assumption (6) will still hold for small enough r. For example, for the 8-bit grayscale images, when $r \leqslant 3$, (6) still hold after right-shifting all of an image's pixels r bits. Therefore, one can right-shift all the pixels $k-1$ bits, and then adopt the estimation equations with $l-k+1$ instead of l to obtain $p_k, p_{k+1}, \dots, p_l$. It can be seen that the equations could have 2 roots for each p_k, $1 \leqslant k \leqslant l$. Then, the root whose absolute value is the least would be selected as the estimation of p_k. And when the equations have no roots in $(-0.05, 0.55)$ (or have no real root), the modification ratios will be viewed as 0.5. By far, the modification ratio in each non-flat pixel's ith bit has been obtained.

Because the MBPIS method converts the image in Gray code into the image in natural binary from higher bit planes to lower bit planes after embedding, the potential modified bits in each non-flat pixel follow

$$\begin{cases} b'_l = g'_l \oplus b_{l+1}, \\ b'_i = g'_i \oplus b'_{i+1}, \quad 1 \leqslant i < l. \end{cases} \tag{27}$$

Thus, the relationship between the modification ratios in Gray code bit planes and natural binary bit planes can be derived as

$$\begin{cases} p_l = p_{GC,l}, \\ p_i = p_{GC,i}(1-p_{i+1}) + (1-p_{GC,i})p_{i+1}, \end{cases} \tag{28}$$

where $p_{GC,i}$ denotes the modification ratio in the ith Gray code bit plane. Then

$$\begin{cases} p_{GC,l} = p_l, \\ p_{GC,i} = (p_i - p_{i+1})/(1-2p_{i+1}). \end{cases} \tag{29}$$

The steganalyzers can compute the modification ratios in Gray code bit planes by (29).

6 Experimental results and analysis

In order to validate the performance of the proposed algorithm, 3075 images downloaded from http://photogallery.nrcs.usda.gov are used to test the algorithm. These images are originally very high resolution color images in format 'tiff', and are then converted into grayscale images in format 'bmp'. Among the images, 40% of them were scaled down to 512×366 pixels, another 40% of them were scaled down to 1024×768 pixels, and the residual images maintained the original size. The MBPIS steganography method was implemented with the familiar threshold $t = 0$, and the bit plane block was with a size of 2×2. Random bits were embedded into the cover images' 3 least significant Gray code bit planes with ratios $p_{GC,i} \in \{0, 0.02, 0.04, 0.06, 0.08, 0.1, 0.15, 0.2, 0.3, 0.35, 0.4\}$, $1 \leqslant i \leqslant 3$. Then, there are 12^3=1728 groups of images, including 1 group of cover images and 1727 groups of stego images, totally 5313600 images. The horizontal and vertical adjacent pixel pairs were utilized in steganalysis, which is a representative option in existing literatures.

It is indicated that [32] when the quantitative steganalysis methods estimate the embedding ratios or modification ratios, the gaps between the estimated values and the real values are usually big, considering that the distribution of estimation error is usually heavy-tailed. And therefore, the median and IQR (interquartile range) are more representative than the familiar mean and standard deviation in evaluating the estimation error of the proposed algorithm. In this paper, we also adopt the median and IQR in evaluating the error of experimental results, and compare the modification ratio estimation accuracy of the proposed algorithm and that of the ID3SPA algorithm presented in [31]. For the reason of space, only part of the experimental results are given as follows.

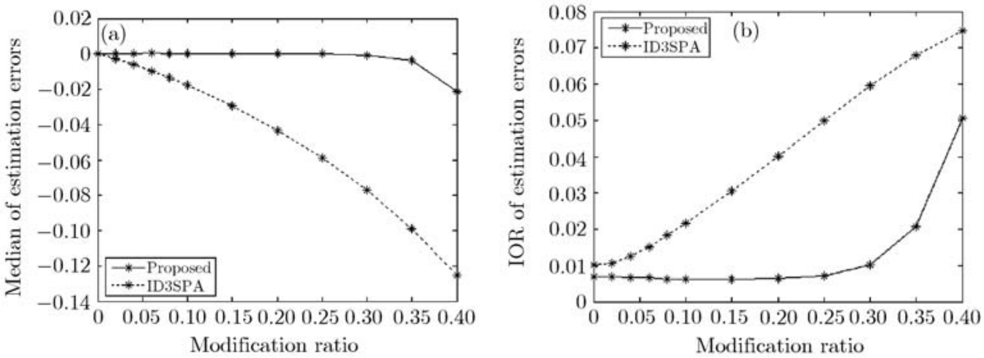

Figure 1 Comparison of estimating the modification ratio in the third Graycode bit plane. (a) Medians of estimation errors; (b) IQRs of estimation errors.

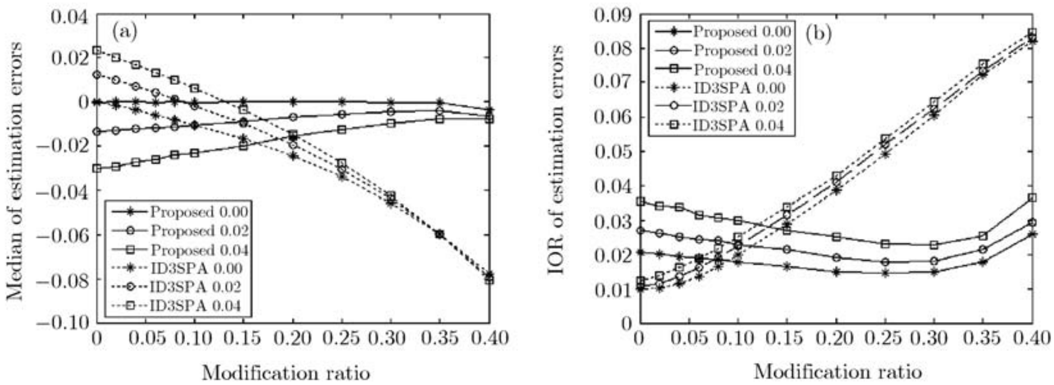

Figure 2 Comparison of estimating the modification ratio in the second Graycode bit plane when $p_{GC,3} \in \{0,\ 0.02,\ 0.04\}$. (a) Medians of estimation errors; (b) IQRs of estimation errors.

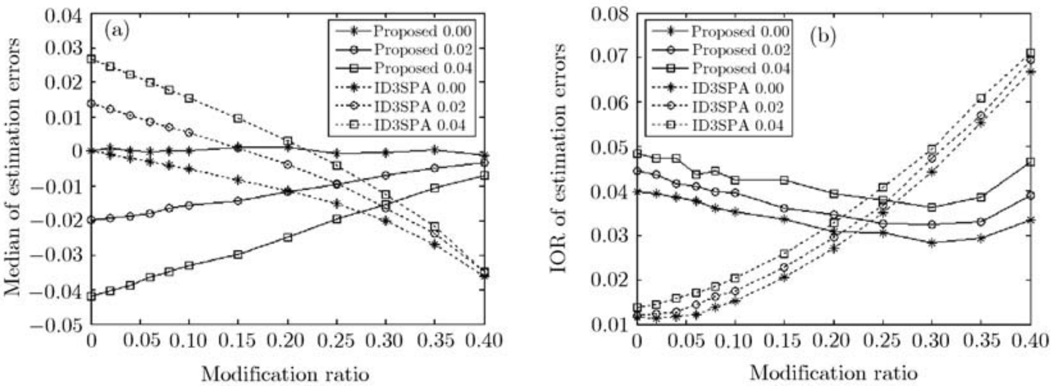

Figure 3 Comparison of estimating the modification ratio in the first Graycode bit plane when $p_{GC,3} = 0$, $p_{GC,2} \in \{0, 0.02, 0.04\}$. (a) Medians of estimation errors; (b) IQRs of estimation errors.

Figure 1 shows the modification ratio estimation errors of the proposed algorithm and the ID3SPA for the third Graycode bit plane. The reason of the difference between two algorithms' estimation errors should be ascribed to the fact that the MBPIS steganography only modifies the pixels in the textured non-flat areas. The ID3SPA algorithm assumes that the steganography modifies randomly all bits in this plane, making the results of ID3SPA on the low side. With the increase of modification ratio, the degree on the low side is increased, and thus, the ID3SPA algorithm is not effective for detecting the MBPIS stego-images. On the contrary, the proposed algorithm considers only the non-flat areas of embedded message, but not flat areas without containing any embedding message. And, this makes the results of proposed algorithm closer to real values in the mass.

Figure 2 shows the estimation errors of the proposed algorithm and ID3SPA for modification ratios in the second Graycode bit plane when the modification ratios in the third Graycode bit plane are $p_{GC,3} \in \{0, 0.02, 0.04\}$. As can be seen, with the rise of modification ratio in the second Graycode bitplane, the estimation errors of the proposed algorithm reduce gradually. Especially, when the modification ratios in the third Graycode bit plane is low, the estimation errors are close to 0 steadily. On the contrary, although the medians of ID3SPA algorithm are comparative with the proposed algorithm when the modification ratio is close to 0, with the increase of modification ratio in the second Graycode bit plane, the estimated modification ratios of ID3SPA are remarkably lower than the practical values. These lower estimated values would affect the identification of stego images seriously. Additionally, with the increase of modification ratio in the third Graycode bit plane, both the amplitudes of the estimation errors of the proposed method and ID3SPA for modification ratio in the second Graycode bit plane become larger, especially when the practical modification ratio in the second Graycode bit plane is low. This issue needs to be studied further.

If the second Graycode bit plane contains secret messages, the results are similar when estimating the modification ratio in the first Graycode bit plane, as shown in Figure 3.

7 Conclusions

In this paper, the problem of adopting the existing quantitative steganalysis method to detect the adaptive steganography is investigated. Firstly, the applicability of the sample pairs analysis model of MLSB replacement steganography for detecting the adaptive steganography is analyzed, and then the conditions of the adaptive steganography that suits to be detected by the model is proposed. For a category of adaptive steganography satisfying the conditions, a general quantitative analysis method is given. And then, for a typical adaptive multiple bit planes image steganography, the modification ratio estimation algorithm is proposed. The experimental results show that the proposed algorithm can estimate the modification ratios of the adaptive multiple bit planes image steganography with high accuracy, and verify the validity of the proposed general quantitative steganalysis method.

It should be noted that, this paper is an elementary exploration on quantitative analysis of adaptive steganography, and there are some other problems yet to be studied, such as the problem of how to ascertain the size of block and the threshold value. At present, some of these problems can be resolved in a certain extent. For instance, for block size $\{2, 3, 4\}\times\{2, 3, 4\}$ in common use, steganalyzers can partition the image into blocks with size of 6×6, and then count the pixel pairs of all 2×2 blocks in four corners to ensure the counted pixel pairs with the two pixels in the same block. However, this skill reduces the availability of pixel pairs. In the next step, we will propose some means to improve the universality and detection accuracy.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 60970141, 60902102, 60873249), the National High-Tech Research & Development Program of China (Grant No. 2008AA10Z419), the Science-Technology Project of Zhengzhou City of China (Grant No. 083SGYG21125), and the Doctoral Dissertation Innovation Fund of Information Science and Technology Institute (Grant No. BSLWCX200804).

References

1 Lian S G, Kanellopoulos D, Ruffo G. Recent advances in multimedia information system security. Inf Sloven Soc Inform, 2009, 33: 3–24

2 Lian S G, Zhang Y. Handbook of Research on Secure Multimedia Distribution. Hershey PA: IGI Global (formerly Idea Group, Inc.), 2009

3 Westfeld A. Detecting low embedding rates. In: Proceedings of 5th International Workshop on Information Hiding, LNCS, vol. 2578. Heidelberg: Springer, 2002. 324–339

4 Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images. IEEE Multimedia, 2001, 8: 22–28

5 Dumitrescu S, Wu X, Wang Z. Detection of LSB steganography via sample pair analysis. IEEE Trans Signal Process, 2003, 51: 1995–2007

6 Fridrich J, Goljan M. On estimation of secret message length in LSB steganography in spatial domain. In: Proceedings of SPIE, Security, Steganography and Watermarking of Multimedia Contents VI, 2004, 5306: 23–34

7 Lu P Z, Luo X Y, Tang Q Y, et al. An improved sample pairs method for detection of LSB embedding. In: Proceedings of 6th International Workshop on Information Hiding, LNCS, vol. 3200. Heidelberg: Springer, 2004. 116–128

8 Ker A. Improved detection of LSB steganography in grayscale images. In: Proceedings of 6th International Workshop on Information Hiding, LNCS, vol. 3200. Heidelberg: Springer, 2004. 97–115

9 Wang G X, Ping X J, Xu M K, et al. Steganalytic method based on short and repeated sequence distance statistics. Sci China Ser F-Inf Sci, 2008, 51: 1466–1474

10 He J H, Huang J W. Steganalysis of stochastic modulation steganography. Sci China Ser F-Inf Sci, 2006, 49: 273–285

11 Fridrich J, Goljan M, Hogea D, Soukal D. Quantitative steganalysis of digital images: estimating the secret message length. ACM Multimedia Syst J, 2003, 9: 288–302

12 Kawaguchi E, Eason R. Principle and applications of BPCS-steganography. In: Proceedings of SPIE, Multimedia Systems and Applications, vol. 3528. New York: SPIE, 1998. 464–472

13 Noda H, Shirazi M, Spaulding J, et al. Application of bit-plane decomposition steganography to JPEG2000 encoded images. IEEE Signal Process Lett, 2002, 9: 410–413

14 Furuta T, Noda H, Niimi M, et al. Bit-plane decomposition steganography using wavelet compressed video. In: Proceedings of forth International Conference on Information, Communications and Signal Processing, vol. 3. Berlin: Singapore, 2003. 970–974

15 Nguyen B, Yoon S, Lee H. Multi bit plane image steganography. In: Proceeding of International Workshop on Digital Watermarking, LNCS, vol. 4283. Berlin: Springer, 2006. 61–70

16 Agaian S, Rodriguez B, Perez J. Stego sensitivity measure and multibit plane based steganography using different color models. In: Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072. New York: SPIE, 2006. 279–290

17 Wang Y, Moulin P. Optimized feature extraction for learning-based image steganalysis. IEEE Trans Inf Foren Secur, 2007, 2: 31–45

18 Luo X Y, Liu F L, Yang C F, et al. Image universal steganalysis based on best wavelet packet decomposition. Sci China Inf Sci, 2010, 53: 634–647

19 Kim C, Chul S, Lee S, et al. Steganalysis on BPCS steganography. In: Pacific Rim Workshop on Digital Steganography, Kitakyushu, Japan, 2003

20 Niimi M, Ei T, Noda H, et al. An attack to BPCS-steganography using complexity histogram and countermeasure. In: Proceedings of International Conference on Image Processing, Singapore, 2004. 733–736

21 Zhang X P, Wang S Z. Statistical analysis against spatial BPCS steganography (in Chinese). J Comput-Aid Design Comput Graph, 2005, 17: 1625–1629

22 Yu X Y, Tan T N, Wang Y H. Reliable detection of BPCS-steganography in natural images. In: Proceedings of the third International Conference on Image and Graphics, Hong Kong, 2004. 333–336

23 Julio L, Raul M, Mariko N, et al. Detection of BPCS-steganography using SMWCF steganalysis and SVM. In: Proceedings of International Symposium on Information Theory and its Applications, Auckland, New Zealand, 2008. 1–5

24 Xuan G R, Shi Y Q, Zou D K, et al. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions. In: Proceedings of International Workshop on Information Hiding, LNCS, vol. 3727. Berlin: Springer, 2005. 262–277

25 Barbier J, Mayoura K. Steganalysis of multi bit plane image steganography. In: Proceedings of International Workshop on Digital Watermarking, LNCS, vol. 5041. Berlin: Springer, 2008. 99–111

26 Yu X Y, Tan T N, Wang Y H. Extended optimization method of LSB steganalysis. In: Proceedings of IEEE International Conference on Image Processing, Genoa, Italy, 2005, 2: 1102–1105

27 Ker A. Steganalysis of embedding in two least-significant bits. IEEE Trans Inf Foren Secur, 2007, 2: 46–54

28 Luo X Y, Yang C F, Wang D S, et al. LTSB steganalysis based on quartic equation. LNCS Trans Data Hid Multimed Secur II, 2007, 4499: 68–90

29 Yu X, Babaguchi N. A fast and effective method to detect multiple least significant bits steganography. In: Proceedings of ACM Symposium on Applied Computing, Ceará, Brazil, 2008. 1443–1447

30 Yang C F, Liu F L, Luo X Y, et al. Steganalysis frameworks of embedding in multiple least-significant bits. IEEE Trans Inf Foren Secur, 2008, 3: 662–672

31 Yang C F, Luo X Y, Liu F L. Embedding ratio estimating for each bit plane of image. In: Proceedings of International Workshop on Information Hiding, LNCS, vol. 5806. Berlin: Springer, 2009, 59–72

32 Böhme R, Ker A. A two-factor error model for quantitative steganalysis. In: Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072. New York: SPIE, 2006. 59–74