A Secure Steganography Preserving High Order Statistics

Guangming Tang
Zhengzhou Information Science and Technology Institute, Zhenghou,China
Email: tgm1983@sina.com

Jing Liu
Zhengzhou Information Science and Technology Institute, Zhenghou, China
Email: kimi_liujing@163.com

Abstract—With the development of steganalysis, the security of steganography is faced with tremendous challenge. High order statistical analysis is an effective and common detecting method that can defeat many hiding scheme. This paper proposes a secure steganography that can effectively resist image steganalysis based on high order statistical analysis. We have analyzed Haar wavelet decomposition characteristics and obtained a theorem about keeping high order statistics invariability. Based on the theorem, the hiding method that can preserve high order statistics of H, V, and D sub-bands of images decomposed by Haar wavelet is devised. In order to strengthen the security of our steganographic scheme, the approach to generate the set of random embedding location is presented. Finally, the capability of proposed algorithm is discussed in theory and proved by experiments. The results show our method possesses perfect imperceptibility and can effectively resist high order statistics analysis and RS analysis.

Index Terms—steganographic algorithm; Haar wavelet decomposition; high order statistics; randomicity

I. INTRODUCTION

Generally speaking, from the view of embedding domain, steganographic algorithm can be categorized as pixel domain embedding (sequential LSB, random LSB, LSB matching etc.) and frequency domain embedding (Outguess, F5 etc.). However, insecurity exists in varying degree in current steganography, for instance, sequential and random LSB can be attacked by RS detection, Chi-square attack and so on. LSB matching can preserve histogram characteristic and F5 can preserve the distribution of DCT coefficients of JPEG blocks, which can escape from Chi-square attack, but the two can’t resist the steganalysis based on high order statistics, which is a representative powerful steganalysis technique.

Many researches on preserving characteristic of statistics have been developed in order to solve the problem of steganography security. For example, Eggers et al. [2] advocated a method that can preserve statistical histogram of image, based on which Tszhoppe et al. [3] advanced a steganographic algorithm based on high order statistics. But these methods only preserve the first or second order statistics of cover image. Once higher order statistical analysis performs on them, their weakness will be discovered. At present, the steganalysis method extracting high order statistics from frequency domain of image to classify can get better results. Like Siwei Lyu et al. [4] built a blind steganalysis model based on the means and high order statistics (variance, skewness, kurtosis) of the frequency coefficients and that of their linear prediction values, which can defeat many common steganographic algorithms, such as LSB, F5 and OutGuess etc. Therefore, there is an urgent requirement to the investigation of steganographic systems that can resist high order statistical analysis. In this paper, based on the analysis of discrete Haar Wavelet, a theory of preserving high-order statistics is obtained, then the theory is utilized for devising a hiding method which can preserve the high order statistics of H, V and D sub-bands of decomposing image. In addition, the method of embedding randomly is employed in the hiding algorithm in order to strengthen security. Theory analysis and experimental results show approving capability of our hiding method.

This paper is organized as follows. In Section 2, the characteristics of decomposition and the statistics preservation of Haar wavelet are analyzed. Then, the new steganographic scheme, including embedding location selection, embedding phase and extracting phase will be presented in Section 3. After that, Section 4 will cover the performance analysis to our algorithm from six aspects, and then the experiment which demonstrate the effectiveness of our proposed method is given in Section 5. Finally, the conclusions will appear in Section 6.

II. DISCRETE HAAR WAVELET

A. Decomposing Characteristics

Haar wavelet presented by Haar at 1910 is so simple, practical and lossless that it gets a broad application in practice. As shown in Fig. 1, for an image \( I_{M \times N} \) \(( M = 0 \bmod 4, N = 0 \bmod 4)\), after decomposed by Haar wavelet with scale two, the wavelet coefficient matrix \( C_{M \times N} \) and \( C_{M \times N}^\prime \) are got, where \( C_{M \times N} \) consists of \( A_{M \times N}^{0,0,0,0} \) \((LL_1)\), \( H_{M \times N}^{0,0,0,0} \) \((HL_1)\), \( V_{M \times N}^{0,0,0,0} \) \((LH_1)\) and \( D_{M \times N}^{0,0,0,0} \) \((HH_1)\), while \( A_{M \times N}^{0,0,0,0} \) \((LL_2)\), \( H_{M \times N}^{0,0,0,0} \) \((HL_2)\), \( V_{M \times N}^{0,0,0,0} \) \((LH_2)\) and \( D_{M \times N}^{0,0,0,0} \) \((HH_2)\) make up of \( C_{M \times N}^\prime \).
From the decomposing characteristics of discrete Haar wavelet, the relation between wavelet coefficients and image pixels is obtained as (1):

\[
\begin{align*}
A^i(j, i) &= 1/4 \left( I(2i - 1, 2j - 1) + I(2i, 2j - 1) \right) \\
H^i(j, i) &= 1/4 \left( I(2i - 1, 2j - 1) + I(2i - 1, 2j) - I(2i, 2j) \right) \\
V^i(j, i) &= 1/4 \left( I(2i, 2j - 1) - I(2i - 1, 2j) \right) \\
D^i(j, i) &= 1/4 \left( I(2i - 1, 2j - 1) - I(2i, 2j) \right)
\end{align*}
\]

(1)

With regard to multiscale image decomposition, the relation is as (2):

\[
\begin{align*}
A^i(j^k, i^k) &= 1/4 \left( A^{i-1}(2^k i^k - 1, 2^k j^k) + A^{i-1}(2^k i^k, 2^k j^k) - A^{i-1}(2^k i^k, 2^k j^k - 1) - A^{i-1}(2^k i^k - 1, 2^k j^k) \right) \\
H^i(j^k, i^k) &= 1/4 \left( A^{i-1}(2^k i^k - 1, 2^k j^k - 1) + A^{i-1}(2^k i^k - 1, 2^k j^k) - A^{i-1}(2^k i^k, 2^k j^k - 1) - A^{i-1}(2^k i^k, 2^k j^k) \right) \\
V^i(j^k, i^k) &= 1/4 \left( A^{i-1}(2^k i^k - 1, 2^k j^k) - A^{i-1}(2^k i^k - 1, 2^k j^k - 1) + A^{i-1}(2^k i^k, 2^k j^k - 1) - A^{i-1}(2^k i^k, 2^k j^k) \right) \\
D^i(j^k, i^k) &= 1/4 \left( A^{i-1}(2^k i^k - 1, 2^k j^k - 1) - A^{i-1}(2^k i^k, 2^k j^k - 1) + A^{i-1}(2^k i^k, 2^k j^k) - A^{i-1}(2^k i^k - 1, 2^k j^k) \right)
\end{align*}
\]

(2)

Where \(i = 1, \ldots, M/2\), \(j = 1, \ldots, N/2\), \(i^k = 1, \ldots, M/2^k\), \(j^k = 1, \ldots, N/2^k\), \(k \geq 2\).

**B. Statistics**

According to (1), mean and high order features are defined for each sub-band of first scale decomposing:

- Mean:

\[
EA^1 = \frac{4}{MN} \sum_{i=1}^{M/2} \sum_{j=1}^{N/2} a_{i,j} = EI,
\]

\[
EH^1 = \frac{4}{MN} \sum_{i=1}^{M/2} \sum_{j=1}^{N/2} h_{i,j},
\]

\[
EV^1 = \frac{4}{MN} \sum_{i=1}^{M/2} \sum_{j=1}^{N/2} v_{i,j},
\]

\[
ED^1 = \frac{4}{MN} \sum_{i=1}^{M/2} \sum_{j=1}^{N/2} d_{i,j},
\]

\[
(3)
\]

Where \(a_{i,j} = A^i(j, i),\ h_{i,j} = H^i(j, i),\ v_{i,j} = V^i(j, i),\ d_{i,j} = D^i(j, i),\)

\(EI\) is the mean of image pixel values.

- High Order Features (\(n \geq 2\)):

\[
STA^n = E \left( a_{i,j} - EA^1 \right)^n,
\]

\[
STH^n = E \left( h_{i,j} - EH^1 \right)^n,
\]

\[
STV^n = E \left( v_{i,j} - EV^1 \right)^n,
\]

\[
STD^n = E \left( d_{i,j} - ED^1 \right)^n.
\]

(4)

Obviously, when \(n = 2, 3, 4\), (4) represents variance, skewness and kurtosis respectively.

According to the analysis of \(a_{i,j}, h_{i,j}, v_{i,j}, d_{i,j}\) \((i = 1, \ldots, M/2, j = 1, \ldots, N/2)\), it’s not difficult to find that the four elements \(I(2i - 1, 2j - 1), I(2i - 1, 2j), I(2i, 2j), I(2i, 2j - 1)\), related to \(a_{i,j}, h_{i,j}, v_{i,j}, d_{i,j}\) can constitute a block with size \(2 \times 2\) in image \(I_{w,n}\). What’s more, the combination of plus and minus operation to these four elements just reflect the characteristics of low-pass, vertical, horizontal and diagonal sub-band. Thus, \(a_{i,j}, h_{i,j}, v_{i,j}, d_{i,j}\), namely the \(2 \times 2\) block, will be regarded as a cell to be analyzed and then a theorem can be gained.

**Theorem 1**: When \(a_{i,j}, h_{i,j}, v_{i,j}, d_{i,j}\) \((i = 1, \ldots, M/2, j = 1, \ldots, N/2)\) keeps consistent before and after embedding, the high order statistics of wavelet coefficients with each scale hold the same.

**PROOF**: Assuming the difference of \(a_{i,j}\) \((i = 1, \ldots, M/2, j = 1, \ldots, N/2)\) before and after embedding is \(b\). The statistic with order \(n (n \geq 2)\) of sub-band \(A_i\) is \(STA^i = E \left( a_{i,j} - EA^1 \right)^n\), while:

\[
EA^i_b = \frac{4}{MN} \sum_{i=1}^{M/2} \sum_{j=1}^{N/2} (a_{i,j} + b) = EA^1 + b
\]

(5)

Namely, when \(a_{i,j}\) is increased by \(b\), the mean \(EA^i\) is also increased by \(b\). Therefore,

\[
STA^i_b = E \left( (a_{i,j} + b) - EA^i_b \right)^n = E \left( (a_{i,j} + b) - (EA^i + b) \right)^n
\]

\[
= E \left( a_{i,j} - EA^i \right)^n = STA^i
\]

(6)
For the sub-band $A_k (k \geq 2)$, according to (2), when $a_{i,j}$ is increased by $b$, then all the coefficients $A^k (j^i,k^i)$ are also increased by $b$. By the same method, we have:

$$\text{STA}^k_i = \text{STA}^k_i$$  \hspace{1cm} (7)

For sub-band H, V and D, the high order statistic invariability also can be proved. Therefore, the theorem is hold.

### III. THE NEW STEGANOGRAPHIC ALGORITHM

From theorem 1, if need to preserve each high order statistic of image discrete Haar wavelet coefficients before and after embedding, then $a_{i,j}, h_{i,j}, v_{i,j}, d_{i,j}$ ($i = 1, \cdots, M/2, j = 1, \cdots, N/2$) of each $2 \times 2$ block must keep consistent in the embedding course. However, because of the randomness of embedded message, it is difficult to assure all of $a_{i,j}, h_{i,j}, v_{i,j}, d_{i,j}$ changeless. In addition, most of current attacks are major in extracting the features of high order statistics of sub-band H, V and D. In view of these problems, in order to preserve the high order features of H, V and D, a new steganographic algorithm which keeps $h_{i,j}, v_{i,j}, d_{i,j}$ after embedding same as that before is presented. In the meanwhile, a method based on randomicity rule is devised to generate the embedding location, which enhances the security further.

#### A. Symbol Specification

- $M^i$: Random secret message stream; the $k^{th}$ message bit $m_k \in \{0,1\}$ and $1 \leq k \leq l$;
- $I_{mnor}$: Cover image with size $n \times m$, where $m = 0 \mod 2, n = 0 \mod 2, m/2 \times n/2 \geq 1$;
- $\text{Brnd}^d$: Embedding block location; the $k^{th}$ block index $\text{brnd}^d_k \in [1,m/2 \times n/2], 1 \leq k \leq l$, and if $k \neq j$, then $\text{brnd}^d_k \neq \text{brnd}^d_j$, where $1 \leq k, k \leq l$;
- $\text{Drnd}^l$: Embedding pixel; the $k^{th}$ embedding pixel in any block $\text{drnd}^l_k \in [1,4], 1 < k < l$;

#### B. Embedding Block Location Generation

Before introducing the generation of block location set for embedding, the following theorem is brought in:

**Theorem 2**: After a random sequence is ascended, its corresponding position index is also a random sequence.

**PROOF**: Define a random sequence $X$, $N$ is the length, and the position index is $i^{As} = \{1,2,\cdots,N\}$. Then any two elements $x_i, x_j$ of $X$ will be denoted by index $k$ with the same probability, namely:

$$P(x_i,k) = P(x_j,k)$$ \hspace{1cm} (8)

Where $x_i, x_j \in X, 1 \leq i, j, k \leq N, i \neq j$.

The relation of sequence and its index is illustrated in Fig. 2.

![Sequence and index relation](image)

If the theorem is false, that means the corresponding position index ($I^{CF} \subset I (I = \{i | 1 \leq i \leq N\})$) of ascended $X$ is un-random. Then there are two elements $i^{As}, j^{As} \in I^{As}$ taking the different probability to appear on index $k^{CF} \in I^{CF}$, namely:

$$P(i^{As},k^{CF}) \neq P(j^{As},k^{CF})$$ \hspace{1cm} (9)

So after ascending, the element $x_{i^{As}} \in X$ denoted by index $i^{As}$ before ascending will appear on index $k^{CF} \in I^{CF}$ with following probability:

$$P(x_{i^{As}},k^{CF}) = P(x_{i^{As}},i^{As})P(i^{As},k^{CF})$$ \hspace{1cm} (10)

Similarly, element $x_{j^{As}} \in X$ will display on index $k^{CF}$ after ascending with the probability of:

$$P(x_{j^{As}},k^{CF}) = P(x_{j^{As}},j^{As})P(j^{As},k^{CF})$$ \hspace{1cm} (11)

According to the characteristics of random sequence $X$, we can get:

$$P(x_{i^{As}},i^{As}) = P(x_{j^{As}}, j^{As})$$ \hspace{1cm} (12)

Then we have:

$$P(x_{i^{As}},k^{CF}) \neq P(x_{j^{As}},k^{CF})$$ \hspace{1cm} (13)

That means, $x_{i^{As}}, x_{j^{As}}$ will appear on index $k^{CF}$ with different probability, which is obviously opposite to the randomicity of $X$. So the hypothesis is false and the theorem is proved.

On the basis of above theorem, an algorithm to generate the set of embedding location is devised as follows:

© 2010 ACADEMY PUBLISHER
• Step1: A stego-key $SD \in (0,1)$ is used as the seed, according to Kent\cite{6} method, a chaotic random sequence $RS$ with the length of $m/2 \times n/2$ is created by iteration. The method as below:

$$r_{s0} = SD, r_{s_{i+1}} = \begin{cases} r_{s_{i}}/\alpha, & \text{if } 0 < r_{s_{i}} < \alpha \\ r_{s_{i}}/(1+\alpha), & \text{if } \alpha \leq r_{s_{i}} < 1 \end{cases}$$ (14)

Where $\alpha = 0.87, \ r_{s_{i}} \in RS, \ 1 \leq i \leq m/2 \times n/2$ .

• Step2: The corresponding position index set $Brand^{PS}$ of ascend $RS$ is taken as the embedding location set. According to theorem 2, set $Brand^{PS}$ is a random sequence. While the length of secret message is $l$, the former $l$ elements of set $Brand^{PS}$ is used as embedding location block set $Brand^{l}$.

C. Hiding Algorithm

• Step1: For secret message bit $m_{k} (1 \leq k \leq l)$ , the embedding block index $brnd_{k}$ is given by $Brnd^{l}$.

Pixels of that block are $I_{1:2i-1,1:j-1},I_{1:2i-1,2j},I_{2i,1:j-1},I_{2i,2j}(i[bmk_{i}/(n/2)], j=brnd_{k}-(i-1)\times n/2)$; 

• Step2: In block $brnd_{k}$, the pixel for embedding is selected by $Drnd^{l}$. And then the corresponding pixel is:

$$I_{k,h} = \begin{cases} I_{2i-1,2j-1}, & \text{if } r_{d_{brnd_{k}}} = 1 \wedge J_{d_{brnd_{k}}} = 1 \\ I_{2i-1,2j}, & \text{if } r_{d_{brnd_{k}}} = 1 \wedge J_{d_{brnd_{k}}} = 2 \\ I_{2i,2j-1}, & \text{if } r_{d_{brnd_{k}}} = 2 \wedge J_{d_{brnd_{k}}} = 1 \\ I_{2i,2j}, & \text{if } r_{d_{brnd_{k}}} = 2 \wedge J_{d_{brnd_{k}}} = 2 \end{cases}$$ (15)

• Step3: Embedding the secret message bit, then the pixels in block $brnd_{k}$ become:

$$I_{r,j} = \begin{cases} I_{r,j} + 1, & \text{if } P_{k,h} \wedge m_{k} \\ I_{r,j} - 1, & \text{if } P_{k,h} \wedge \neg m_{k} \\ I_{r,j}, & \text{else} \end{cases}$$ (16)

(2i-1 \leq i \leq 2i, \ 2j-1 \leq j \leq 2j) \quad \text{and} \quad P_{k,h} = \begin{cases} 1, & \text{if } I_{k,h} \mod 2 = 1 \\ 0, & \text{if } I_{k,h} \mod 2 = 0 \end{cases}

Namely:

1) If $m_{k} = 1$ and $I_{k,h}$ is even, then all the pixels in $brnd_{k}$ are added by 1.

2) If $m_{k} = 0$ and $I_{k,h}$ is odd, then all the pixels in $brnd_{k}$ are subtracted by 1.

3) If $m_{k} = 1$ and $I_{k,h}$ is odd, or $m_{k} = 0$ and $I_{k,h}$ is even, all the pixels keep the same.

• Step4: $k = k + 1$ , repeat step1, for all the secret bits are embedded.

D. Extracting Algorithm

• Step1: According to $Brnd^{l}$, the embedding block $brnd_{k}$ for $k$ th $1 \leq k \leq l$ bit is obtained.

• Step2: In virtue of $Drnd^{l}$, the extracting pixel $d_{r,j}$ and its value in block $brnd_{k}$ is got.

• Step3: Extracting the message bit:

$$m_{k} = \begin{cases} 1, & \text{if } P_{k,h} = 1 \\ 0, & \text{if } P_{k,h} = 0 \end{cases}$$ (17)

Namely if $I_{k,h}$ is odd, then $m_{k} = 1$; if $I_{k,h}$ is even, then $m_{k} = 0$;

• Step4: $k = k + 1$ , repeat Step1 for all the secret message are extracted.

IV. ALGORITHM ANALYSIS

A. High Order Statistics Preservation

For every $2 \times 2$ block of cover image, three situations will happen to the pixel values:

a) All are added by one, then:

$$a_{i,j} = \frac{1}{4} \left( (I(2i-1,2j-1)+1) + (I(2i-1,2j)+1) + (I(2i,2j-1)+1) + (I(2i,2j)+1) \right) $$

$$ = a_{i,j} + 1 \quad (18)$$

b) All are subtracted by one, then:

$$h_{i,j} = \frac{1}{4} \left( (I(2i-1,2j-1)-1) - (I(2i-1,2j)+1) - (I(2i,2j-1)-1) + (I(2i,2j)+1) \right) $$

$$ = h_{i,j} \quad (18)$$

b) All are subtracted by one, then:

$$d_{i,j} = \frac{1}{4} \left( (I(2i-1,2j-1)-1) + (I(2i-1,2j)+1) - (I(2i,2j-1)-1) - (I(2i,2j)+1) \right) $$

$$ = d_{i,j}$$

b) All are subtracted by one, then:

$$a_{i,j} = a_{i,j} - 1, \quad h_{i,j} = h_{i,j}, \quad v_{i,j} = v_{i,j}, \quad d_{i,j} = d_{i,j}$$ (19)
According to a), b), c), after discrete Haar wavelet decomposition, the sub-band H, V and D coefficients of cover image keep the same. According to the theorem 1, the means and high order statistics of H, V and D are also invariable. However, the statistics of sub-band A are changed to some degree, which is still puniness and has little impact to steganographic security. Generally speaking, information hiding is similar to add some noise to the cover image, which will have great effect to sub-band H, V and D. Therefore, to a certain extent, steganographic security can be assured by the preservation of decomposed image’s high order statistics.

B. Pixel Movement

For the pixel $I_{k_i,k_j}$ used for embedding message bit, there are three movements too:

1) If $I_{k_i,k_j}$ is even and the embedding message bit is 1, then $I_{k_i,k_j}$ is added by one;

2) If $I_{k_i,k_j}$ is odd and the embedding message bit is 0, then $I_{k_i,k_j}$ is subtracted by one;

3) $I_{k_i,k_j}$ keeps the same if other situations;

Obviously, for a gray image with pixel range of $[0, 255]$, the embedding method wouldn’t result in overflow of pixel. For example, considering the two pixel poles 0 and 255: pixel 0 either keeps the same or becomes 1 while pixel 255 either keeps the same or becomes 254. This embedding manner can guarantee to extract the embedded message integrally.

C. Complexity

The time complexity is $O(1)$, which is connected with the length of embedded message. The space complexity is $O(mn+\ell)$. The complexity of brute force search is $O(2^{mn})$.

It can be seen that the time and space complexity are linear and the complexity of brute force search is decided by the length of embedded message and the size of cover image. That means: even if the embedding action is detected, the attacker should compute $[m/2\times n/2]/[m/2\times n/2-\ell]$ times in order to extract all the secret message bits. When the length of embedded message achieves to the maximal capacity, this number is so enormous that the extraction is impossible under current condition. Thus, the algorithm can stand against extracting attack as well.

D. Embedding Capacity

Because each block only embeds one bit message, the maximal embedding capacity of this embedding method is $m/2\times n/2$, which is $1/4$ of that of LSB embedding algorithm.

E. Imperceptibility

When the whole least plan of $I_{mn}$ is used for embedding, the PSNR can achieve the minimal:

$$PSNR_{\min} = 10\log_{10}\left(\max\left(\frac{1}{\ell}\right)\right)$$

In practice, setting $\max\left(\frac{1}{\ell}\right) = 255^2$ usually, so the PSNR of our method here is $PSNR_{\min} = 48.1308$ db, which is much larger than the threshold of 39 db. Therefore, the algorithm can perform fine imperceptibility.

F. Steganographic Security

The proposed algorithm like LSB matching either adds or subtracts one from all pixels of the block. This strategy can keep the histogram approximate before and after embedding, so it can resist RS attack; And the idea that the block with the size of $2 \times 2$ is regarded as the minimal cell for embedding can save the relativity of local pixels and can make some detection based on relativity prediction of pixels failed. So the algorithm can defeat some current spatial steganalysis. Because of the preservation of high order statistics based on Haar wavelet decomposition, the algorithm also can resist the steganalysis in DWT domain. In addition, the generation of embedding location set follows the principle of randomicity, which can strengthen the security comparatively.
From Fig. 3 and Fig. 4, it can be seen that no matter what kinds of image, the change by our algorithm is litter. We can’t tell the difference between original and stego image. In addition, the PSNR of each image is larger than 46db and keeps about 50db, so we can conclude that the human visual characteristics are preserved perfectly, meeting the requirement of visual imperceptibility.

B. High Order Statistics Preservation Experiment

Based on theorem 1 and analysis in the beginning of Section 3, the aim of our algorithm is only to keep the statistics invariability of sub-band H, V and D because of the difficulty of preserving the statistics of all the sub-bands. So, the statistics of sub-band A will change.

Just as the analysis above, in the experiment, the algorithm preserves the means and high order statistics of sub-band H, V and D of image discrete Haar wavelet decomposition, and that of sub-band A change in some degree.

Due to page length limitation, we only give the case of sub-band A. Fig. 5 shows the mean, variance, skewness and kurtosis difference of sub-band A before and after embedding. From Fig. 5, the majority of statistics of sub-band A are keeps round of 0, and the change of mean, skewness and kurtosis are litter. Although the change of variance is obvious, the change is unordered.
C. High Order Statistical Analysis Test

In order to test our algorithm’s capability of resisting high order statistical analysis, sequence LSB and LSB matching are selected to be compared with our algorithm. The steganalysis method proposed by [4] is utilized to attack these three schemes. The embedding rate is 1, and the embedded message is the bit sequence of 01, following the discrete uniformity random distribution. The detection rate DR, false rate FR and negative rate NR are shown as Table I.

<table>
<thead>
<tr>
<th>Hiding Method</th>
<th>Detecting Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DR (%)</td>
</tr>
<tr>
<td>Sequence LSB</td>
<td>83.68</td>
</tr>
<tr>
<td>LSB matching</td>
<td>74.32</td>
</tr>
<tr>
<td>Our algorithm</td>
<td>66.25</td>
</tr>
</tbody>
</table>

Obviously, referring to resist high order statistical attack, our algorithm performs better than sequence LSB and LSB matching. This advantage agrees with above analysis completely. It is mainly determined by the devising goal that the algorithm should preserve high order statistics of image discrete Haar wavelet decomposition coefficients. What’s more, the embedding manner that using $2^2$ block as the elementary embedding cell can preserve the relativity of local pixel areas in a certain extent. Therefore, the difference between original and stego image of our method is smaller than that of the other two hiding algorithms, and the capability of resisting attack is self-evident.

D. RS Steganalysis Test

Our algorithm is a spatial steganography, while RS analysis is an effective steganalysis technique utilizing sensitive dual statistics derived from spatial correlations. In order to test the spatial correlation preservation of our method, RS analysis is used to perform on the stego image generated by our algorithm.

In this experiment, the range of confidence of $R$ is set as $[0.9515, 1.0315]$, while that of $S$ is $[0.9635, 1.0635]$. Such set can get a higher false rate but lower negative rate and be convenient for the analysis of the algorithm security.

From Fig. 6, it is apparent that only 12 images (red points) are out of the range of confidence. That means just 0.995% of the stego images used in our experiment can be detected by RS analysis, while other 99.05% of stego images can resist RS analysis successfully. Therefore, the algorithm proposed in this paper can defeat RS steganalysis effectively.

VI. CONCLUSION

In this paper, the decomposing characteristics of discrete Haar wavelet and the condition for keeping high order statistics invariability are researched, and a method to generate random embedding location is presented, and then a spatial steganographic algorithm preserving high order statistics of discrete Haar wavelet decomposition coefficients is devised. The statistics invariability and security of the algorithm are analyzed in theory. Experimental results indicate that the proposed method with satisfactory imperceptibility has the capability of resisting RS analysis and steganalysis based on high order statistics. However, the algorithm is devised on the basis of Haar wavelet decomposition, which will limit the application to other wavelet decomposition. But the idea of how to construct such algorithm can inspire the presentation of much more normal steganographic algorithms resisting high order statistical analysis. According to theorem 1, each $2^2$ block should have consistent change for preserving the high order statistics of Haar wavelet decomposition. Considering other wavelet, the relativity between wavelet coefficients and image pixel blocks can be gained by analyzing the decomposition characteristic. Take DB8 wavelet decomposition as an example. Any of its wavelet coefficients is relative to a $5 \times 5$ pixel block of image. And then some strategy can be implemented to make the embedding change consistent. Consequently, the aim of preserving the high order statistics can be achieved. Finally, the steganographic algorithm can be devised by the strategy.

REFERENCES


Guangming Tang was born in Wuhan, China in 1963. She received the B.S., M.S. and Ph.D. degrees in information security from Zhengzhou Information Science and Technology Institute, Henan, China, in 1983, 1990, and 2008, respectively.

She is presently a Professor with the department of Information Security, Information Engineering University, Henan, China. Her fields of professional interest are information hiding, watermarking and software reliability. She has published 49 research articles and 3 books in these areas.

Ms. Tang is a recipient of Provincial Prize for Progress in Science and Technology.

Jing Liu was born in Xuancheng, China in 1985. She received the B.S. degree from Zhengzhou Information Science and Technology Institute, Henan, in 2007.

Currently, she is pursuing the M.S. degree in information security at Zhengzhou Information Science and Technology Institute. Her research interest includes information hiding and information security.