第 34 卷 第 17 期 计 算 机 工 程 2008 年 9 月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0149—04 文献标识码：A 中图分类号：TP309

一种保持频域高阶统计特征不变的隐写算法

张石树，汤光明
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：在分析离散 Haar 小波分解特性的基础上，论证保持其高阶统计特征不变性引理，据此设计一种空域隐写算法，保持了图像 Haar 小波分解后 H、V、D 区域的高阶统计特征。该算法使嵌入信息满足不可见性，具有一定抗 RS 攻击和基于高阶统计特征检测的能力，为构造保持高阶统计特征不变的更一般性隐写算法提供了一种启发式思路。

关键词：隐写算法；Haar 小波分解；高阶统计特征

Steganograph Algorithm on Preservation of High Order Statistics in Frequency Domain

ZHANG Shi-shu, TANG Guang-ming
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 This paper proves a lemma of how to preserve high order statistics based on analyzing the decomposition characters of discrete Haar wavelet. According to this lemma, it proposes a spatial steganograph algorithm. It can preserve high order statistics of H, V and D areas, and make embedded messages sightless. Experimental results show that it can effectively resist RS attack. It arises some inspiration for constructing better steganograph methods to preserve high order statistics.

【Key words】 steganograph algorithm; Haar wavelet decomposition; high order statistics

1 概述

目前，隐写算法根据嵌入域一般分为空域替换法和频域变换法。空域替换法主要有连续LSB、随机LSBLSB匹配等嵌入法；而频域变换法主要有OutGuess, F5[1]。但现有隐写算法都存在或多或少的安全风险，如连续LSB、随机LSB算法可遭到RS检测、直方图卡方攻击。虽然LSB匹配算法基本保持了宿主图像直方图的一阶统计特征，F5 算法近似保持了JPEG图像分块DCT系数的统计分布，可避免卡方攻击，但两者仍抵抗不了基于高阶统计特征的隐写检测攻击。

针对保持统计特征的隐写算法，学者们也进行了一番深入研究。如文献[2]提出了保持图像统计直方图的隐写算法；文献[3]在其基础上提出了一种基于高阶统计量的隐写算法。但这些大多仅保持了宿主图像的一阶或 二阶统计特征，在更高阶统计特征上仍存在较大差别，给隐写算法的安全带来了不确定性。而且，从频域提取区分宿主图像的高阶统计特征来分析隐写算法，可取得较好的检测效果。如文献[4]采用频域系数及其线性预测值的均值和高阶统计量(如方差、偏度、峭度)对 LSB, F5, OutGuess 等常用隐写算法进行了有效的隐写盲检测。这样，研究一种能够保持频域高阶统计特征的隐写算法迫在眉睫。

本文在分析离散 Haar 小波分解特性的基础上，提出并证明保持其高阶统计特征不变性引理和一种空域隐写算法。

2 离散 Haar 小波

2.1 分解特性

Haar小波是 1910 年由Haar提出的。它简单、实用，且变换、还原后无任何信息损失，在工程中得到了广泛的应用。在信息隐藏中，可采用Haar小波对图像进行多分辨率分析；在Haar小波频域内嵌入水印信息进行数字版权保护，提取图像特征进行隐写分析等。对于图像 $I_{M\times N}$ ($M\equiv 0 \bmod 4$，$N\equiv 0 \bmod 4$)，采用离散Haar小波对其二级分解后，得到小波系数矩阵 $\boldsymbol{C}^1_{M\times N}$，$\boldsymbol{C}^2_{M\times N}$。其中，$\boldsymbol{C}^1_{M\times N}$ 由 $A^1_{M/2\times N/2}$ (LL_1区)、$H^1_{M/2\times N/2}$ (HL_1区)、$V^1_{M/2\times N/2}$ (LH_1区)、$D^1_{M/2\times N/2}$ (HH_1区)构成；同样，$\boldsymbol{C}^2_{M\times N}$ 由 $A^2_{M/4\times N/4}$ (LL_2区)、$H^2_{M/4\times N/4}$ (HL_2区)、$V^2_{M/4\times N/4}$ (LH_2区)、$D^2_{M/4\times N/4}$ (HH_2区)组成，见图 1。

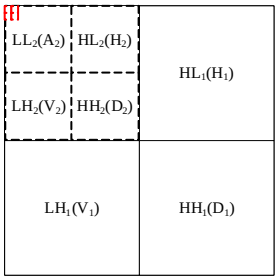


图 1 离散 Haar 小波二级分解示意图

通过分析离散Haar小波的分解特性[5]知，小波系数与图像数据的对应关系如下：

$$\begin{cases} A^1(j,i)=1/4\big(I(2i-1,2j-1)+I(2i-1,2j)+I(2i,2j-1)+I(2i,2j)\big) \\ H^1(j,i)=1/4\big(I(2i-1,2j-1)+I(2i-1,2j)-I(2i,2j-1)-I(2i,2j)\big) \\ V^1(j,i)=1/4\big(I(2i-1,2j-1)-I(2i-1,2j)+I(2i,2j-1)-I(2i,2j)\big) \\ D^1(j,i)=1/4\big(I(2i-1,2j-1)-I(2i-1,2j)-I(2i,2j-1)+I(2i,2j)\big) \end{cases} \tag{1}$$

若进行多级分解，则 2 级以上的系数满足

作者简介：张石树(1982－)，男，硕士研究生，主研方向：信息隐藏；汤光明，教授

收稿日期：2007-09-15 **E-mail：**zhangss_2@163.com

$$\begin{cases} A^k(j^k,i^k)=1/4\left(A^{k-1}(2i^k-1,2j^k-1)+A^{k-1}(2i^k-1,2j')+A^{k-1}(2i^k,2j^k-1)+A^{k-1}(2i^k,2j^k)\right) \\ H^k(j^k,i^k)=1/4\left(A^{k-1}(2i^k-1,2j^k-1)+A^{k-1}(2i^k-1,2j')-A^{k-1}(2i^k,2j^k-1)-A^{k-1}(2i^k,2j^k)\right) \\ V^k(j^k,i^k)=1/4\left(A^{k-1}(2i^k-1,2j^k-1)-A^{k-1}(2i^k-1,2j')+A^{k-1}(2i^k,2j^k-1)-A^{k-1}(2i^k,2j^k)\right) \\ D^k(j^k,i^k)=1/4\left(A^{k-1}(2i^k-1,2j^k-1)-A^{k-1}(2i^k-1,2j')-A^{k-1}(2i^k,2j^k-1)+A^{k-1}(2i^k,2j^k)\right) \end{cases} \tag{2}$$

其中，(i=1,2,⋯,M/2; j=1,2,⋯,n/2; i^k=1,2,⋯,$M/2^k$; j^k=1,2,⋯,$n/2^k$, $k\geq 2$)。

2.2 统计特征

根据式(1)，对一级分解中各区域分别定义均值(mean)、高阶统计量(high order features)，则有

(1)均值

$$EA^1=\frac{4}{MN}\sum_{i=1}^{M/2}\sum_{j=1}^{N/2}a_{i,j}=EI \tag{3}$$

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

$$EV^1=\frac{4}{MN}\sum_{i=1}^{M/2}\sum_{j=1}^{N/2}v_{i,j} \tag{5}$$

$$ED^1=\frac{4}{MN}\sum_{i=1}^{M/2}\sum_{j=1}^{N/2}d_{i,j} \tag{6}$$

其中，$a_{i,j}=A^1(j,i)$；$h_{i,j}=H^1(j,i)$；$v_{i,j}=V^1(j,i)$；$d_{i,j}=D^1(j,i)$；EI 为图像的像素均值。

(2)高阶统计量($n\geq 2$)

$$STA^1=E\left(a_{i,j}-EA^1\right)^n \tag{7}$$

$$STH^1=E\left(h_{i,j}-EH^1\right)^n \tag{8}$$

$$STV^1=E\left(v_{i,j}-EV^1\right)^n \tag{9}$$

$$STD^1=E\left(d_{i,j}-ED^1\right)^n \tag{10}$$

显然，当 $n=2,3,4$ 时，分别代表了统计量：方差(variance)，偏度(skewness)，峭度(kurtosis)。

分析 $a_{i,j}$, $h_{i,j}$, $v_{i,j}$, $d_{i,j}$ ($i=1,2,\cdots,M/2$, $j=1,2,\cdots,N/2$)发现，其中 4 个元素 $I(2i-1,2j-1)$, $I(2i-1,2j)$, $I(2i,2j-1)$, $I(2i,2j)$ 为图像 $I_{M\times N}$ 中分割相邻的 2×2 小方块；而它们为这 4 个元素加减运算的 4 种组合，反映了小块的低频、水平高频、垂直高频、对角高频 4 组特征。现在，将 $a_{i,j}$, $h_{i,j}$, $v_{i,j}$, $d_{i,j}$ (即 2×2 的小单元块)作为一个小整体来分析，可得：

引理 当 $a_{i,j}$ (或 $h_{i,j}$, $v_{i,j}$, $d_{i,j}$)(i=1,2,⋯,M/2, $j=1,2,\cdots,N/2$) 变化一致时，其对应所有级分解系数的高阶统计量不变。

证明

设 $a_{i,j}$ ($i=1,2,\cdots,M/2$, $j=1,2,\cdots,N/2$)的变化量均为b，区域A_1对应的n ($n\geq 2$)阶统计量为 $STA^1=E\left(a_{i,j}-EA^1\right)^n$。

而 $EA_b^1=\frac{4}{MN}\sum_{i=1}^{M/2}\sum_{j=1}^{N/2}\left(a_{i,j}+b\right)=EA^1+b$。那么，当各 $a_{i,j}$ 增加 b 时，相应的均值 EA^1 增加为 b。因此

$$STA_a^1=E\left(\left(a_{i,j}+b\right)-EA_a^1\right)^n=E\left(\left(a_{i,j}+b\right)-\left(EA^1+b\right)\right)^n=$$
$$E\left(a_{i,j}-EA^1\right)^n=STA^1$$

对于A_k区域(一级以上分解)，由式(2)可知，当各 $a_{i,j}$ 增加b时，其中所有的系数 $A^k(j^k,i^k)$ 同样增加b。同理可证明 $STA_a^k=STA^k$。

对于 H, V, D 区域，同理可证明其高阶统计特征不变，即引理成立。

证毕。

3 保持 Haar 小波分解高阶统计特征的隐写算法

由引理知，若要保持隐写前后图像经离散 Haar 小波分解后的各高阶统计量不变，则需在隐写过程中确保各 2×2 小块的 $a_{i,j}$, $h_{i,j}$, $v_{i,j}$, $d_{i,j}$ 变化一致。而在实际隐写中，由于嵌入消息的随机性，很难保证嵌入时各小块 $a_{i,j}$, $h_{i,j}$, $v_{i,j}$, $d_{i,j}$ 的增减一致。而且隐写分析者主要从 H, V, D 区域提取高阶统计特征来攻击隐写算法。针对这些问题，本文提出一种新的隐写策略，使嵌入后各小块 $a_{i,j}$, $v_{i,j}$, $d_{i,j}$ 不变，从而保持宿主载体隐写前后 H, V, D 区域的高阶统计特征。

3.1 符号说明

M^l：随机信息序列($m_k\in\{0,1\}$，$1\leq k\leq l$)；

$I_{m\times n}$：$n\times m$ 大小的宿主图像($m\equiv 0 \bmod 2$，$n\equiv 0 \bmod 2$，$m/2\times n/2\geq l$)；

$Brnd^l$：嵌入块位置随机选择信息($brnd_k\in[1,m/2\times n/2]$，$1\leq k\leq l$；$brnd_{k_i}\neq brnd_{k_j}\left(\text{if } k_i\neq k_j\right), 1\leq k_i,k_j\leq l$)；

$Drnd^l$：嵌入点位置随机选择信息($drnd_k\in[1,4]$，$1\leq k\leq l$)；

3.2 嵌入策略

Step1 选取信息位 m_k ($1\leq k\leq l$)，根据 $Brnd^l$ 得到其嵌入块位置 $brnd_k$；此时块中对应的像素值分别为

$$\left\{I_{2i-1,2j-1},I_{2i-1,2j},I_{2i,2j-1},I_{2i,2j}\right\}$$
$$i=\lceil brnd_k/(n/2)\rceil$$
$$j=brnd_k-(i-1)\times n/2$$

Step2 然后在 $brnd_k$ 块中，由 $Drnd^l$ 选择嵌入点 $drnd_k$；则对应的像素值

$$I_{i_k,j_k}=\begin{cases} I_{2i-1,2j-1} & \text{if } I_{drnd_k}=1\wedge J_{drnd_k}=1 \\ I_{2i-1,2j} & \text{if } I_{drnd_k}=1\wedge J_{drnd_k}=2 \\ I_{2i,2j-1} & \text{if } I_{drnd_k}=2\wedge J_{drnd_k}=1 \\ I_{2i,2j} & \text{if } I_{drnd_k}=2\wedge J_{drnd_k}=2 \end{cases} \tag{11}$$

其中，$I_{drnd_k}=\lceil drnd_k/2\rceil$；$J_{drnd_k}=\left(drnd_k-2\left(\lceil drnd_k/2\rceil-1\right)\right)$。

Step3
$$I_{i',j'}=\begin{cases} I_{i',j'}+1 & \text{if } \left(\sim P_{I_{i_k,j_k}}\wedge m_i\right) \\ I_{i',j'}-1 & \text{if } \left(P_{I_{i_k,j_k}}\wedge \sim m_i\right) \\ I_{i',j'} & \text{else} \end{cases} \tag{12}$$

其中，$2i-1\leq i'\leq 2i$；$2j-1\leq j'\leq 2j$；$P_{I_{i_k,j_k}}=\begin{cases}1 & \text{if } I_{i_k,j_k} \bmod 2=1\\ 0 & \text{if } I_{i_k,j_k} \bmod 2=0\end{cases}$。

(1)若 $m_k=1$ 且 I_{i_k,j_k} 为偶数，则 $drnd_k$ 块中所有像素值加 1；

(2)若 $m_k=0$ 且 I_{i_k,j_k} 为奇数，则 $drnd_k$ 块中所有像素值减 1；

(3)若 $m_k=1$ 且 I_{i_k,j_k} 为奇数，或 $m_k=0$ 且 I_{i_k,j_k} 为偶数，则 $drnd_k$ 块中所有像素值不变。

Step4 $k=k+1$，转 Step1，直到长度为 l bit 的信息全部嵌入完毕。

3.3 提取策略

Step1 根据 $Brnd^l$ 得到第 k ($1\leq k\leq l$) bit 嵌入块位置 $brnd_k$；

Step2 由 $Drnd^l$ 在块 $brnd_k$ 中获取提取点 $drnd_k$，由此得到像素值 I_{i_k,j_k}；

Step3 $m_k=\begin{cases}1 & \text{if } P_{I_{i_k,j_k}}=1\\ 0 & \text{if } P_{I_{i_k,j_k}}=0\end{cases}$；即若 I_{i_k,j_k} 为奇数，则 $m_k=1$；

若 I_{i_k,j_k} 为偶数，则 $m_k=0$ ；

Step4 $k=k+1$，转 Step1，直到所有位的信息提取完毕。

3.4 算法分析

(1)Haar 小波分解高阶统计特征不变性

对于宿主图像中的每 2×2 的小块，其像素值将出现下列 3 种情况：

1)集体增 1

$$a'_{i,j}=\frac{1}{4}((I(2i-1,2j-1)+1)+(I(2i-1,2j)+1)+(I(2i,2j-1)+1)+(I(2i,2j)+1))=a_{i,j}+1$$

$$h'_{i,j}=\frac{1}{4}((I(2i-1,2j-1)+1)+(I(2i-1,2j)+1)-(I(2i,2j-1)+1)-(I(2i,2j)+1))=h_{i,j}$$

$$v'_{i,j}=\frac{1}{4}(I(2i-1,2j-1)+1)-(I(2i-1,2j)+1)+(I(2i,2j-1)+1)-(I(2i,2j)+1)=v_{i,j}$$

$$d'_{i,j}=\frac{1}{4}(I(2i-1,2j-1)+1)-(I(2i-1,2j)+1)-(I(2i,2j-1)+1)+(I(2i,2j)+1)=d_{i,j}$$

2)集体减 1，同理可得 $a'_{i,j}=a_{i,j}-1$，$h'_{i,j}=h_{i,j}$，$v'_{i,j}=v_{i,j}$，$d'_{i,j}=d_{i,j}$ ；

3)集体不变，$a'_{i,j}=a_{i,j}$，$h'_{i,j}=h_{i,j}$，$v'_{i,j}=v_{i,j}$，$d'_{i,j}=d_{i,j}$。

根据 3 种情况，明显，宿主图像经离散 Haar 小波变换后其 H, V, D 区域的系数值均不变；进一步结合引理可知，其相应 H, V, D 各区域的均值及高阶统计量均不变；而 A 区域的相关统计量有了一定程度的改变。但这种改变量甚微，对隐写安全性危害较小。一般信息嵌入，相当于对原始载体叠加部分噪声，对 H, V, D 区域的影响较大，而保持这些部分高阶统计特征有着一定的隐写安全性。因此，该算法满足一定的隐写安全性需求。

(2)嵌入点像素值 I_{i_k,j_k} 的 3 种变化

1)如果为偶数，而嵌入信息为 1，则增 1；

2)如果为奇数，而嵌入信息为 0，则减 1；

3)剩余情况，保持不变。

对于灰度图像(像素值为 $[0,255]$)，这种嵌入方式显然不会造成像素值的溢出。例如，考虑灰度图像的 2 个极值 0 和 255：0 要么不变，要么增 1 成 1；而 255 要么不变，要么减 1 为 254。这样可确保嵌入的信息被完整提取。

(3)相关复杂度

时间复杂度为 $O(l)$，仅与嵌入信息的长度有关；空间复杂度为 $O(m\times n+3l)$ ；若 $Brnd^l$，$Drnd^l$ 由相关随机种子产生，则空间复杂度减为 $O(m\times n+l)$ ；穷尽复杂度为 $O(l^{mn})$。显然，其时间、空间复杂度为线性时间，穷尽复杂度由嵌入信息长度和宿主图像大小决定，可抵抗蛮力破解。

(4)最大嵌入容量为 $m/2\times n/2$ bit，为 LSB 嵌入算法的 $1/4$ ；这主要由其每小块嵌入 1 bit 信息所致。

(5)不可见性

本算法中，当 $I_{m\times n}$ 整个平面变化时，其 PSNR 值最小，不难算出 $PSNR_{\min}=10\lg\left(\max\left(I^2_{m\times n}\right)\right)$。实际中一般设置 $\max\left(I^2_{m\times n}\right)=255^2$，那么，此时本算法的 $PSNR_{\min}=48.130\ 8$ dB，远大于阈值 39 dB，不可见性较好。

(6)隐写安全性

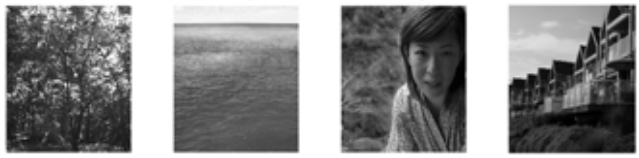
算法采用整小块加 1、减 1 嵌入策略，类似于 LSB 匹配的嵌入原理，使得隐写前后直方图规律基本不变，可抵抗 RS 攻击；同时由于其改变的最小单元为 2×2 小块，保持了局部像素间的相关性，在一定程度上使得基于像素间相关性预测检测失效。因此，针对现有的空域隐写检测手段，该算法有着一定的隐写安全性。进一步，该算法保持了基于 Haar 小波分解的高阶统计特征，对 DWT 域隐写分析起到了一定的抵抗作用。

3.5 实验分析

宿主载体来源于图像库Groundtruth[6]和Greenspun[7]，将其统一从中心裁剪成 1 206 幅大小为 400×400 的 8 位灰度图像，并编号为 1~1 206，包括人物、风景、建筑等内容。而嵌入的信息设置为最大嵌入容量，为 40 000 bit。

(1)嵌入和提取效果

在图 2 中，4 个原始图像的 bpm 从左到右分别为 003, 101, 1 049 和 345；4 个隐写图像的 PSNR 从左到右分别为 51.148 3, 51.072 9, 51.131 9 和 51.065 8。从图 2、图 3 可见，不论是树木、山河，还是人物、建筑等图像，采用本算法对其改变较小，*PSNR* 值都大于 46 dB，且基本保持在 50 dB 左右，远比阈值 39 dB 大，很好地保持了宿主图像的视觉特征，满足隐藏信息视觉不可见性要求。



(a)原始图像



(b)隐写图像

图 2 图像隐写效果

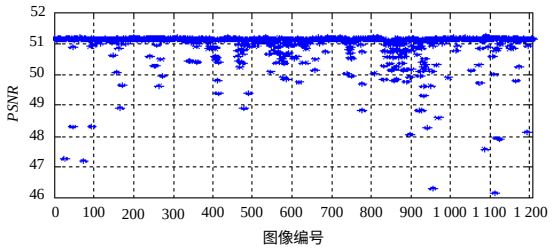


图 3 图像隐写后的 PSNR 值

(2)高阶统计特征保持

实验结果正如理论分析的那样，本算法保持了宿主图像经过离散 Haar 小波分解后 H, V, D 区域的均值及高阶统计特征，而 A 区域有一定程度的变化。由于篇幅所限，图 4 仅给出了原始图像和载秘图像分别经离散 Haar 小波一级分解后，A 区域均值、方差、偏度和峭度的偏差。A 区域各统计值绝大部分保持在 0 水平线上，其中均值、偏度、峭度变化甚小，方差虽然有一定的变化，但无规律性。

(3)高阶统计特征攻击

对于连续 LSB、LSB 匹配及本文算法，统一采取文献[4]提出的用频域高阶统计特征来区分原始图像和载秘图像。其嵌入率设置为 100%，嵌入信息为离散均匀随机分布的 01 bit 序列。而检测率 *DR*、误检率 *FD* 和漏检率 *ND* 如表 1 所示。

表 1　高阶统计特征攻击检测对比　(%)

	DR	*FD*	*ND*
连续 LSB	83.68	7.05	9.27
LSB 匹配	74.32	11.37	14.31
本文算法	66.25	13.18	20.57

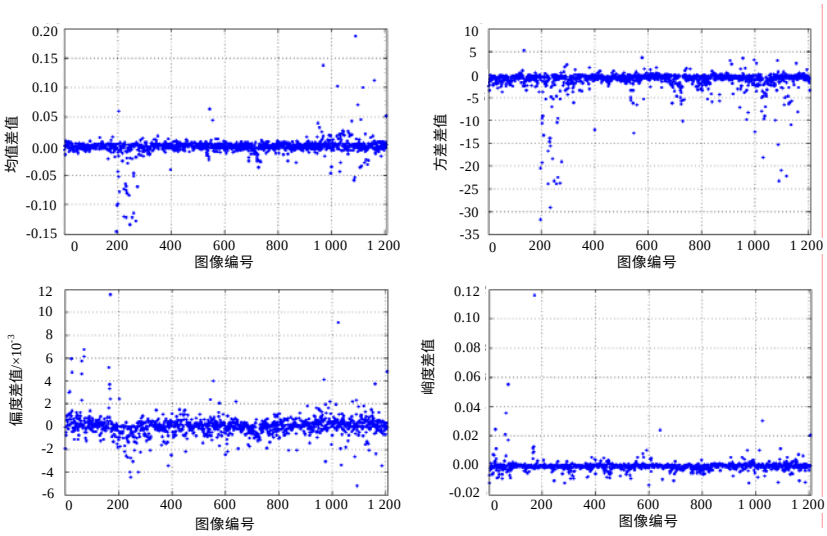


图 4　原始图像和载秘图像 DWT 域 A 区域统计特征差

本算法在抗高阶统计特征攻击方面明显优于连续 LSB 和 LSB 匹配算法。这主要是因为本算法以保持宿主图像经离散 Haar 小波分解后高阶统计特征不变性为设计目标，以整 2×2 小块为嵌入的基本单元，在一定程度上保持了局部像素区域的相关性。这样，其原始图像和载秘图像像素间相关性差别要低于其他 2 种隐写算法，抗攻击的能力自然不言而喻。

(4)RS 检测攻击

RS 检测分析中，R 的置信区间设置为[0.951 5,1.031 5]，S 的置信区间为[0.963 5,1.063 5]。这样设置虽然使得检测的误报率较高，但可使检测的漏报率较低，有利于分析本算法的安全性，见图 5。

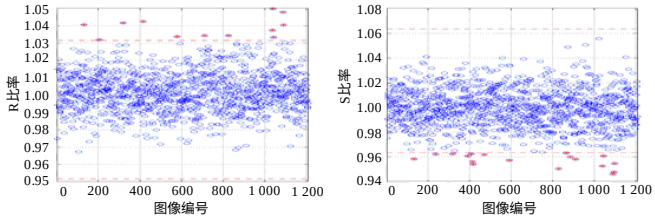


图 5　RS检测分析中R比率和S比率

从图 5 可知，在 1 206 幅图像中，仅有 12 幅(右下方)不在置信区间内，也就是说在实验图像库中，本算法按最大容量嵌入后仅有 0.995%能被 RS 检测到，而其余 99.005%的隐写图像能躲避 RS 的攻击。因此，本算法具有较好抗 RS 攻击的能力。

4　结束语

本文通过研究离散 Haar 小波的分解特性及其高阶统计特征不变性原理，提出了一种图像离散 Haar 小波分解后高阶统计特征保持不变的空域隐写算法。该算法能保证隐藏信息的不可见性，具有一定抗 RS 攻击和基于高阶统计特征检测的能力。然而此算法只能保持离散 Haar 小波分解的高阶统计特征，针对其他小波分解则可能存在一定的局限性。但其整个构造过程可为提出更一般性的保持频域高阶统计特征的隐写算法打开了思路。由引理可知，要保持 Haar 小波分解高阶统计特征，则需各 2×2 小块的变化一致。对于其他小波，可先分析其分解特性，获取小波系数与图像像素块间的相关性。比如，对于 DB8 小波分解，其一个小波系数与图像中 5×5 的小块相关。然后，采用某种策略使各块的变化一致，从而达到保持小波分解后高阶统计特征不变的目的。最后，根据这种策略来制定具体的隐写算法。

参考文献

[1] 王朔中, 张新鹏, 张开文. 数字密写和密写分析－－互联网时代的信息战技术[M]. 北京: 清华大学出版社, 2005-04.

[2] Eggers J J, Bauml R, Gorod B. A Communications Approach to Image Steganography[C]//Proceedings of Conf. on Security and Watermarking of Multimedia Contents IV. San Jose, CA, USA: [s. n.], 2002.

[3] Tzschoppe R, Bauml R, Huber J B, et al. Steganographic System Based on Higher-order Statistics[C]//Proceedings of Conf. on Security and Watermarking of Multimedia Contents V. Santa Clara, California, USA: [s. n.], 2003.

[4] Lyu S, Farid H. Steganalysis Using Higher-order Image Statistics[J]. IEEE Transactions on Information Forensiscs and Security, 2006, 1(1): 111-119.

[5] 孙延奎. 小波分析及其应用[M]. 北京: 机械工业出版社, 2005.

[6] Greenspun Image Database[Z]. (1997-04-04). http://philip.greenspun.com/.

[7] Groundtruth Image Database[Z]. (2004-08-08). http://www.cs.Washington.edu/research/imagedatabase/groundtruth/UniveofWashington.

（上接第 148 页）

[2] Li Chuanming, Hwang T, Lee N Y. Remark on the Threshold RSA Signature Scheme[C]//Proc. of Advances in Cryptology-CRYPRO'93. Berlin, Germany: Springer, 1994: 413-420.

[3] Gan Yuanju. Verifiable Threshold Signature Schemes Against Conspiracy Attack[J]. Journal of Zhejiang University Science, 2004, 5(1): 50-54.

[4] Xie Qi. Cryptanalysis and Improvement of Two Threshold Signature Schemes[J]. Journal on Communications, 2005, 26(7): 123-128.

[5] Li Chuanming, Hwang T, Lee N Y. Threshold Multisignature Schemes Where Suspected Forgery Implies Traceability of Adversarial Shareholders[C]//Proc. of EUROCRYPT'94. [S. l.]: Springer, 1995: 194-204.

[6] Michels M, Horster P. On the Risk of Disruption in Several Multiparty Signatures Schemes[C]//Proc. of Advances in Cryptology-ASIACRYPT'96. Berlin, Germany: Springer, 1996: 334-345.