图像 Hadamard 变换域鲁棒水印算法

张大兴[1,2],李何明[1],李海华[1]
ZHANG Da-xing[1,2],LI He-ming[1],LI Hai-hua[1]

1.杭州电子科技大学 图形图像研究所,杭州 310018
2.浙江大学 CAD & CG 国家重点实验室,杭州 310027
1.Institute of Graphics and Image,Hangzhou Dianzi University,Hangzhou 310018,China
2.State Key Lab of CAD & CG,Zhejiang University,Hangzhou 310027,China
E-mail:dxzhang@cad.zju.edu.cn

ZHANG Da-xing,LI He-ming,LI Hai-hua.Robust image watermarking algorithm in Hadamard domain.Computer Engineering and Applications,2010,46(5):76-79.

Abstract: This paper proposes a new robust watermarking algorithm based on block Hadamard Transform(HT).The binary watermark image is displaced to destroy space relativity and then expanded to get watermark sequence.The original image is subdivided to 8×8 blocks and is executed HT transform.Then middle HT coefficients are selected to hide watermark.The correlation of watermark code and the difference of HT coefficients between embedded and original image is used to determine each bit when watermark is detected.Experiment shows that the algorithm has no appreciable influence to image appearance and it is robust to JPEG compression,clipping,filtering and noise pollution.

Key words: digital watermark;Hadamard transform;robust watermark

摘 要:提出了一种基于分块 Hadamard 变换的鲁棒图像水印算法。水印图像先进行置乱和扩展得到水印序列。原始图像进行 8×8 分块的 Hadamard 变换,在中频系数里按不同强度嵌入水印。水印提取时,先计算与原始图像在对应的变换域系数的差值,再计算该差值与水印编码的相关性来确定每个水印像素。实验表明,该算法对原始图像的视觉影响小,具有良好的鲁棒性。

关键词:数字水印;Hadamard 变换;鲁棒水印
DOI:10.3778/j.issn.1002-8331.2010.05.023 **文章编号**:1002-8331(2010)05-0076-04 **文献标识码**:A **中图分类号**:TP391.41

1 引言

数字水印是研究在宿主数字媒体(图像、音频、视频)中隐藏特定信息的技术。根据原始载体不同,可分为图像水印、音频水印、视频水印等;根据隐藏位置不同,可分为空域水印和变换域水印;根据水印生存性,可分为鲁棒水印和脆弱水印。早期的数字水印技术集中在空域,典型代表 LSB 算法[1],虽然实现简单,但隐藏数据量较少,且抗几何攻击和信号处理操作的鲁棒性较差。目前,变换域算法由于对视觉影响小,鲁棒性好而受到研究者的重视。主要的变换域包括:离散余弦变换(DCT)[2-4],离散傅里叶变换(DFT)[5-6],离散小波变换(DWT)[7-8],哈达玛变换(Hadamard Transform,HT)[9-13]等。Cox 等人提出的一种基于DCT变换的扩频水印技术[2],该算法抗信号处理能力较强,但对几何攻击比较敏感。而利用 DFT 变换的旋转和缩放的不变特性,DFT 域的水印对几何失真具有很好的鲁棒性[5-6],但 DFT 变换要用到复数乘法,所以计算比较复杂。而更为复杂的傅里叶-梅林变换(Fourier-Merlin transform)[14]和对数极坐标变换(log-polar transform)[15]虽然抗几何攻击和信号处理操作的鲁棒性都比较好,但计算代价太大。现在的水印算法中,DWT 用的比较多,比如把原始图像分成 4 个子带,并分别应用奇异值分解(SVD),通过修改奇异值来嵌入水印[8],该算法抗几何攻击和信号处理操作的鲁棒性较好。而 HT 具有正逆变换相同、速度快、计算简单等优点。文献[9]提出了一种基于 HT 的水印算法,该算法先把原图分块变换为 HT 系数,并选择一些块中的系数来嵌入水印数据,算法对信号处理操作具有较强的鲁棒性,同时也能抗一部分几何攻击。

在灰度图像中嵌入一个较小的二值图像作为水印信息,研究算法的鲁棒性、视觉不可察觉性。

2 图像的 Hadamard 变换

对于变换域水印,时频变换过程在整个水印算法中占主要部分。水印算法中常用的变换操作如 DFT 和 DCT 变换的快速算法要用到复数乘法,水印嵌入过程通常会耗时十几分钟甚至更多(即使研究用的 256×256 Lena 小尺寸图像耗时几分钟也不少见)。HT 变换过程存储空间小,运算速度快,在图像处理和

基金项目:浙江省自然科学基金(the Natural Science Foundation of Zhejiang Province of China under Grant No.Y105278)。
作者简介:张大兴(1971-),男,副教授,主要研究方向为数字图像处理、密码学和信息安全;李何明(1982-),男,主要研究方向为数字图像处理;李海华(1983-),男,主要研究方向为数字图像处理。
收稿日期:2008-08-20 **修回日期**:2008-12-25

图像压缩领域已经得到广泛应用。令[U]代表源图像，[V]代表经过变换后的图像，二维 HT 如下：

$$[V]=\frac{\boldsymbol{H}_n[U]\boldsymbol{H}_n}{N} \tag{1}$$

式(1)中 $\boldsymbol{H}_n$ 代表一个 $N\times N$ 的 HT 矩阵，$N=2^n$，$n=1,2,\cdots$。

HT 矩阵具有如下性质：

$$\boldsymbol{H}_n=\boldsymbol{H}_n^*=\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{H}^{-1} \tag{2}$$

n 级的 HT 矩阵可以由 $n-1$ 级矩阵使用 Kronercker 乘积⊗来实现：

$$\boldsymbol{H}_n=\boldsymbol{H}_{n-1}\otimes\boldsymbol{H}_1 \text{ 或 } \boldsymbol{H}_n=\begin{bmatrix}\boldsymbol{H}_{n-1} & \boldsymbol{H}_{n-1}\\ \boldsymbol{H}_{n-1} & -\boldsymbol{H}_{n-1}\end{bmatrix} \tag{3}$$

3　水印嵌入算法

3.1　水印图像预处理

水印图像的预处理分为两个过程，即置乱和编码。

置乱操作可以消除图像像素的空间相关性。设二值水印图像大小为 $W\times W$，具体的置乱方法为：

(1)将 1 到 $W\times W$ 的整数序列根据密钥 Key 进行置乱，得到伪随机序列 P；

(2)设该序列的第 n 个元素是 Pn，令：$n=k*W+l$；$Pn=i*W+j$；

(3)交换像素位置：将原始水印的像素(i,j)放到新位置(k,l)，即完成水印的置乱处理。

对水印图像的每个像素进行扩展编码可以增强算法的鲁棒性，像素值的编码用 wj_k 表示，j 的取值为 0 或 1 代表二值图像中的像素数值，下标 k 代表编码的每个二进制位。采用 24 位二进制互补编码，$w0_k$ 用编码 101010101010101010101010 表示(像素值 0)，$w1_k$ 用 010101010101010101010101 表示(像素值 1)，这样编码后两者具有最大的距离，在后续水印提取时的相关性也更明确，因此 k 的取值为 1 到 24。这样完整的水印信息可以用 $w_{i,k}$ 来表示，i 表示水印图像的第 i 个像素，范围是 1 到 $W\times W$，k 则表示该像素扩展后的第 k 个二进制位。

水印二值图像的大小为 32×32。这样水印总的信息量为 32×32×24=24 576 bit。

3.2　原始图像预处理

对图像进行分块操作，作为后续在每个分块中嵌入一个水印像素的预处理。设原始图像的大小为 $M\times N$，则可以划分为 $(M/8)\times(N/8)$个互不重叠的 8×8 的子块。一般 M 和 N 远大于 W，所以子块的个数要远大于水印图像的像素数目，因此可以对水印像素进行重复嵌入或者选择部分子块来进行嵌入，采用后者。具体步骤为：

(1)计算子块/像素比$((M/8)\times(N/8))/(W\times W)$，以小于等于该数值的最大整数作为选择因子 R；即从每 R 个子块中选择一个子块用来隐藏一个水印像素。

(2)设原始图像为 $I=\{f(x,y),0\leqslant x\leqslant M,0\leqslant y\leqslant N\}$，则从原始图像中得到的$(M/8)\times(N/8)$个 8×8 子块分别为：$B(m,n)=\{f(8*m+i,8*n+j),0\leqslant i,j\leqslant 7\}$，其中，$0\leqslant m\leqslant M/8$，$0\leqslant n\leqslant N/8$。

3.3　Hadamard 变换和水印的嵌入

由于纹理复杂的图像块比平坦块具有更好的视觉掩蔽特性，因此水印嵌入的强度可以大一些，纹理信息会在变换域系数中体现出来，一般纹理丰富的子块其变换域系数的数值变化范围也相对较大。在 Hadamard 变换的中频系数中加入水印，具体的过程为：

(1)对选中的子块进行 Hadamard 变换：$p_{i,k}=HT(B_i)$，i 表示选中嵌入水印的第 i 个子块，k 是变换后的系数序号，取值为 1 到 64。

(2)对 8×8 系数矩阵按 Zigzag 进行排序后，选取中间 24 个系数用于嵌入水印。

(3)计算中间 8 个系数的最大值和最小值的平均值 $mean$ 来确定水印强度系数 α，目的是使水印强度和纹理复杂度建立联系。具体计算公式如下：

$$\alpha=\begin{cases}0.5, & \text{if } mean<1\\ 1.0, & \text{if } 1\leqslant mean<2\\ 1.5, & \text{if } mean\geqslant 2\end{cases} \tag{4}$$

(4)在第 i 个子块的 24 个中频系数中嵌入水印：

$$p'_{i,k}=p_{i,k}+\alpha\cdot\mathrm{sign}(w_{i,k}-0.5),i=1,2,\cdots,W\times W;k=1,2,\cdots,24 \tag{5}$$

(5)对选中的子块进行 Hadamard 逆变换，最终得到含水印图像。

水印的嵌入过程归纳起来如图 1 所示。

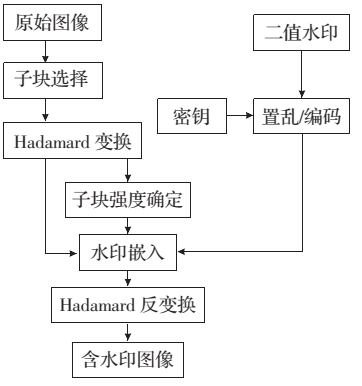


图 1　水印嵌入流程图

4　水印的提取

提取水印时需要原始图像，水印的提取过程如图 2 所示，具体的过程如下：

(1)把含水印图像和原始图像分别划分为 8×8 的子块。

(2)分别对含水印的图像子块和原始图像中对应的子块进行 Hadamard 变换。

(3)仍然按照前述相同的方法取出原始图像和含水印图像子块对应的 24 个中频变换系数，求两者差值得到 $p_{i,k}$。

(4)将 $p_{i,k}$ 与水印像素的 0 和 1 编码进行相关性计算。公式如下：

$$C(j)_i=\rho(p_{i,k},wj_k)=\frac{\sum_{k=1}^{24}p_{i,k}wj_k}{\sqrt{\sum_{k=1}^{24}(p_{i,k})^2}\cdot\sqrt{\sum_{k=1}^{24}(wj_k)^2}}$$

$$i=1,2\cdots,W\times W;j=0,1 \tag{6}$$

比较 $C(0)_i$ 和 $C(1)_i$ 的大小确定第 i 个子块嵌入的是 0 还是 1。

$$w_i=\begin{cases}0,\text{if } C(0)_i\geqslant C(1)_i\\ 1,\text{if } C(0)_i<C(1)_i\end{cases}\quad i=1,2,\cdots,W\times W \tag{7}$$

(5)w_i 反置乱后重建得到二值水印图像。

计算提取的水印与原始水印之间的相似性进行水印算法的性能评估。相似性计算公式为：

$$NC=\rho(w,w^*)=\frac{\sum_{i=1}^{32}\sum_{j=1}^{32}w(i,j)w^*(i,j)}{\sqrt{\sum_{k=1}^{32}\sum_{j=1}^{32}w^2(i,j)}\cdot\sqrt{\sum_{k=1}^{32}\sum_{j=1}^{32}w^{*2}(i,j)}} \tag{8}$$

原始水印为 W,提取水印为 W^*,相似性数据在 0 和 1 之间,其值越大说明图像包含水印的可能性越大。

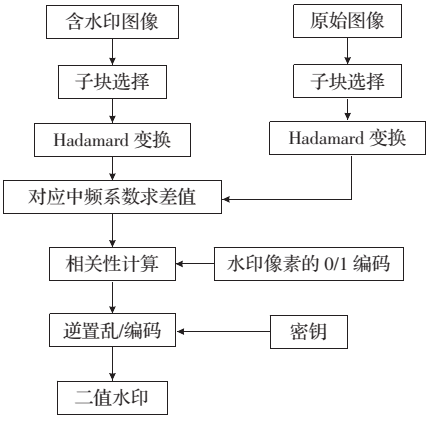


图 2 水印提取流程图

5 实验结果

实验结果是在 Matalab6.5 平台下仿真得到的。原始图像是 Lena 灰度图像(大小是 512×512),水印图像是 32×32 的二值图。

5.1 水印视觉影响

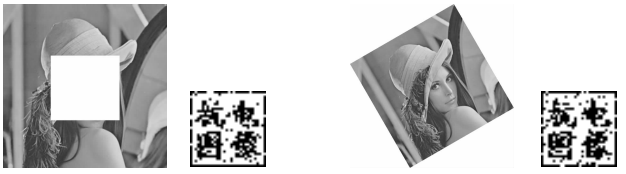
原始图像、二值水印图、含水印图像和提取出的二值水印图分别如图 3(a)~图 3(d)所示。由图 3 中可以看出,水印的嵌入没有对原始图像造成可察觉的影响,具有良好的不可感知性。

(a)原始图像(512×512) (b)原始水印 (c)含水印图像(*PSNR*=45.58) (d)提取的水印

图 3 水印视觉影响比较图

5.2 几何攻击鲁棒性测试和比较

图像经常会进行各种几何操作,如缩放、旋转、平移以及各种组合操作,图 4 是图像受几何攻击后提取水印的部分效果图,表明算法对各种几何攻击有很好的鲁棒性。该文与文献[4]中的算法对比实验,文献[4]中的算法是基于分块的 DCT 域的非盲算法,为了更精确地比较,用该文的二值水印图替换算法中的水印序列。表 1 是具体的相关性数据以及和对比算法的比较,算法在鲁棒性方面有比较明显的优势。



(a)剪切后图像及提取的水印(几何剪切 25%,提取的水印相似度=0.849 7) (b)旋转攻击后图像及提取的水印(旋转 30°后恢复,提取的水印相似度=0.900 0)

图 4 几何攻击的鲁棒性测试

5.3 信号处理攻击鲁棒性测试和比较

信号处理是图像的另一种常见操作,如滤波、加噪、压缩等。图 5 是图像受信号处理攻击后提取水印的部分效果图,表明算法对各种信号处理有很好的鲁棒性。表 2 是具体的相关性数据以及和其他算法的比较。算法在鲁棒性方面和文献[4]相比有比较明显的优势。

表 1 几何攻击鲁棒性测试和比较数据

攻击类型		文献[4]		该文	
		PSNR/dB	NC	PSNR/dB	NC
直接提取		41.108 4	1.000 0	45.577 4	1.000 0
几何剪切	几何剪切 5%	20.964 1	0.950 5	22.390 5	0.981 0
	几何剪切 10%	17.455 2	0.892 5	18.603 1	0.960 8
	几何剪切 25%	12.166 0	0.796 9	13.499 0	0.849 7
涂改	涂改 5%	17.576 9	0.931 0	18.237 4	0.961 4
	涂改 10%	15.324 4	0.894 7	15.704 3	0.937 8
	涂改 25%	13.139 5	0.845 2	14.548 8	0.889 3
旋转	旋转 10°	27.043 9	0.739 2	29.869 1	0.848 2
	旋转 20°	28.577 6	0.811 7	29.925 2	0.855 3
	旋转 30°	28.841 5	0.812 0	30.384 4	0.900 0
平移	水平平移 10 像素	22.633 1	0.959 8	22.584 1	0.981 1
	水平平移 20 像素	19.532 9	0.942 5	19.464 1	0.973 3
	水平平移 50 像素	15.420 6	0.883 6	15.342 1	0.943 4
缩放	缩放比例 0.5	33.762 1	0.503 1	42.354 0	0.996 4
	缩放比例 0.9	35.797 2	0.421 4	40.793 6	1.000 0
	缩放比例 2.0	37.201 9	0.504 0	41.962 3	1.000 0
组合攻击	旋转 10°和平移 10 像素	27.336 8	0.819 2	28.072 6	0.820 2
	旋转 20°和平移 20 像素	26.087 1	0.810 9	26.576 9	0.825 1
	旋转 30°和平移 50 像素	22.721 8	0.806 6	22.791 5	0.820 5

(c)压缩攻击后图像及提取的水印(压缩质量因子 Q=70,提取的水印相似度=0.998 8) (d)滤波攻击后图像及提取的水印(中值滤波,提取的水印相似度=0.925 7)

图 5 信号处理攻击的鲁棒性测试

表 2 信号处理攻击的鲁棒性测试和比较数据

攻击类型		文献[4]		该文	
		PSNR/dB	NC	PSNR/dB	NC
直接提取		41.108 4	1.000 0	45.577 4	1.000 0
滤波	中值滤波	35.172 8	0.915 9	42.174 7	0.925 7
	均值滤波	34.627 3	0.911 8	34.625 7	0.912 2
JPEG 压缩	JPEG 压缩(*Quality*=70)	36.345 2	0.972 1	42.450 6	0.998 8
	JPEG 压缩(*Quality*=60)	35.729 6	0.964 9	41.407 1	0.984 4
	JPEG 压缩(*Quality*=50)	35.273 1	0.961 7	40.526 4	0.930 6
	JPEG 压缩(*Quality*=40)	34.764 4	0.922 8	39.507 7	0.830 0
椒盐噪声	椒盐噪声(密度 0.01)	25.392 0	0.829 2	25.653 8	0.958 3
	椒盐噪声(密度 0.05)	18.568 4	0.589 8	18.603 1	0.824 6
	椒盐噪声(密度 0.1)	15.526 6	0.525 9	15.558 9	0.700 4
高斯噪声	高斯噪声(均值 0,方差 0.003)	25.108 3	0.749 5	25.182 4	0.906 0
	高斯噪声(均值 0,方差 0.01)	20.011 1	0.634 0	20.032 0	0.751 3
	高斯噪声(均值 0,方差 0.1)	11.210 6	0.502 0	11.245 0	0.603 8
乘性噪声	乘性噪声(均值 0,方差 0.01)	25.107 2	0.771 0	25.212 0	0.915 7
	乘性噪声(均值 0,方差 0.05)	18.320 8	0.590 3	18.379 2	0.710 2
	乘性噪声(均值 0,方差 0.1)	15.431 6	0.511 9	15.531 0	0.647 1

此外,对算法的速度进行了量化测试和比较。相比于文献[4]中的算法,在每比特图像数据加水印速度方面具有十分明显的优势。

6 结论

提出的 Hadamard 变换域鲁棒水印算法,不但能够同时抵抗几何攻击和信号处理攻击,提取高度相关的水印,具有良好的鲁棒性,水印对图像视觉外观无明显的影响,而且在速度上也有优势,算法可以应用于版权保护等应用领域。

参考文献:

[1] van Schyndel R G,Tirkel A Z,Osborne C F.A digital watermark[C]//IEEE International Conference on Image Processing,Austin,Texas,USA,1994:86-90.

[2] Cox I J.Secure spread spectrum watermarking for multimedia[J].IEEE Transaction on Image Processing,1997,6(12):1673-1687.

[3] Yu Peng-fei,Liu Bing.Public watermarking algorithm based on the polarity of DCT coefficients[C]//6th International Conference on Intelligent Systems Design and Applications(ISDA2006),Jinan,China,2006:277-282.

[4] 黄继武,Shi Y Q,程卫东.DCT 域图像水印:嵌入对策和算法[J].电子学报,2000,28(4):57-60.

[5] Solachidis V,Pitas I.Circularly symmetric watermark embedding in 2D DFT domain[J].IEEE Transaction on Image Proeessing,2001,10(11):1741-1753.

[6] 王向阳,郜俊,侯丽敏.一种基于图像特征点的数字水印嵌入方法[J].电子学报,2007,35(7):1318-1322.

[7] 李智,陈孝威.小波和余弦变换相结合的灰度图像水印算法[J].中国图象图形学报,2006,11(6):834-839.

[8] Ganic E,Eskicioglu A M.Robust DWT-SVD domain image watermarking:Embedding data in all frequencies[C]//Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security,Magdeburg,Germany,2004:166-174.

[9] Ho A T S,Shen Jun,Chow A K K,et al.Robust digital image-in-image watermarking algorithm using the fast Hadamrd transform[C]//Proceedings of the 2003 International Symposium on Circuits and Systems,Bangkok,Thailand,2003:826-829.

[10] Ruhurdju S,Xie Shou-lie.An algorithm to compute unified complex Hadamard transform[C]//7th International Symposium on Signal Processing and Its Applications,Paris,France,2003:173-176.

[11] Fonda F,Pastore S.Innovative image watermarking tecnique for image authentication in surveillance applications[C]//International Workshop on Imaging Systems and Techniques(IST 2005),Canada,2005:32-35.

[12] Abdallah E E,Hamza A B,Bhattacharya P.A robust block-based image watermarking scheme using fast Hadamard transform and singular value decomposition[C]//The 18th International Conference on Pattern Recognition(ICPR'06),Hong Kong,2006:673-676.

[13] Falkowski B J.Multi-polarity complex Hadamard transforms for phase watermarking algorithm[C]//2007 6th International Conference on Information,Communications & Signal Processing,2007:1-5.

[14] Ruanaidh J J K Ó,Pun T.Rotation,scale and translation invariant spread spectrum digital image watermarking[J].Signal Processing,1998,66(3):303-317.

[15] Wang Bin,Han Guo-qiang,Huang Jun-cai,et al.A robust blind algorithm for color image watermarking[C]//IEEE International Conference on Control and Automation(ICCA 2007),Guangzhou,China,2007:142-146.

(上接 32 页)

证明 由定理 2.6 知 $v_f(1)=\cdots=v_f(2k-1)=v_f(2k+1)+1=\cdots=v_f(4k-1)+1$,$v(f+\sigma_1)=(v_f(0),v_f(1)+1,v_f(2),\cdots,v_f(4k-1)+1,v_f(4k))=(v_f(0),v_f(4k-1),\cdots,v_f(1),v_f(4k))=v(f(xA))$,其中 A 为每一行每一列均有 $n-1$ 个 1 的可逆矩阵。而 $AI(f(xA))=AI(f)$[8]。所以命题成立。

3 结论

变元个数 n 为奇数或者 2^m 时,具有最大代数免疫度对称函数的个数和代数标准型都已确定。结论可用于减少前人搜索 AI 达到最大的 $2k$ 元对称函数的算法的运算量;另一方,当 n 为其他特殊形态如 2^m-2 时,为代数免疫度达到最大的对称函数的个数和形态的完全确定奠定了基础。

参考文献:

[1] Courtois N,Meier W.Algebraic attacks on stream ciphers with linear feedback[C]//LNCS 2656:Advances in Cryptology-EUROCRYPT 2003.Berlin:Springer-Verlag,2003.

[2] Courtois N.Fast algebraic attacks on stream ciphers with linear feedback[C]//LNCS 2729:Advances in Cryptology-CRYPTO 2003.Berlin:Springer-Verlag,2003:176-194.

[3] Armknecht F.Improving fast algebraic attacks[C]//LNCS 3017:FSE 2004.Berlin:Springer-Verlag,2004:65-82.

[4] Batten L M.Algebraic attacks over $GF(q)$[C]//LNCS 3348:Progress in Cryptology-INDOCRYPT 2004.Berlin:Springer-Verlag,2004:84-91.

[5] Meier W,Pasalic E,Carlet C.Algebraic attacks and decomposition of Boolean function[C]//LNCS 3027:Advances in Cryptology-EUROCRYPT 2004.Berlin:Springer-Verlag,2004:474-491.

[6] Dalai D K,Maitra S,Sarkar S.Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J/OL].Design Code Cryptog,2006,40(1):41-58.http://eprint.iacr.org/2005/229.

[7] Li N,Qi W F.Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity[J].IEEE Trans Inf Theory,2006,52(5):2271-2811.

[8] Braeken A,Preneel B.On the algebraic immunity of symmetric Boolean functions[C]//LNCS 3797:INDOCRYPT 2005.[S.l.]:Springer-Verlag,2005:35-48.

[9] Liu F,Feng K.Efficient computation of algebraic immunity of symmetric Boolean functions[M]//LNCS 4484:Theory and Applications of Models of Computation.Berlin:Springer,2007:318-329.

[10] 冯克勤,廖群英.对称布尔函数的代数免疫性[J].工程数学学报,2008,25(2):191-198.

[11] Carlet C,Dalai D K,Gupta K C,et al.Algebraic immunity for cryptographically significant Boolean functions:Analysis and construction[J].IEEE Trans Inf Theory,2006,52(7):3105-3121.

[12] Canteaut A,Videau M.Symmetric Boolean functions[J].IEEE Trans Inf Theory,2005,51(8):2791-2811.

[13] Qu L J,Li C,Feng K Q.A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables[J].IEEE Trans Inf Theory,2007,53(8):2908-2910.

[14] Qu L J,Li C.On the 2^m-variable symmetric Boolean functions with maximum algebraic immunity[J].Sci China Ser F-Inf Sci,2008,51(2):120-127.