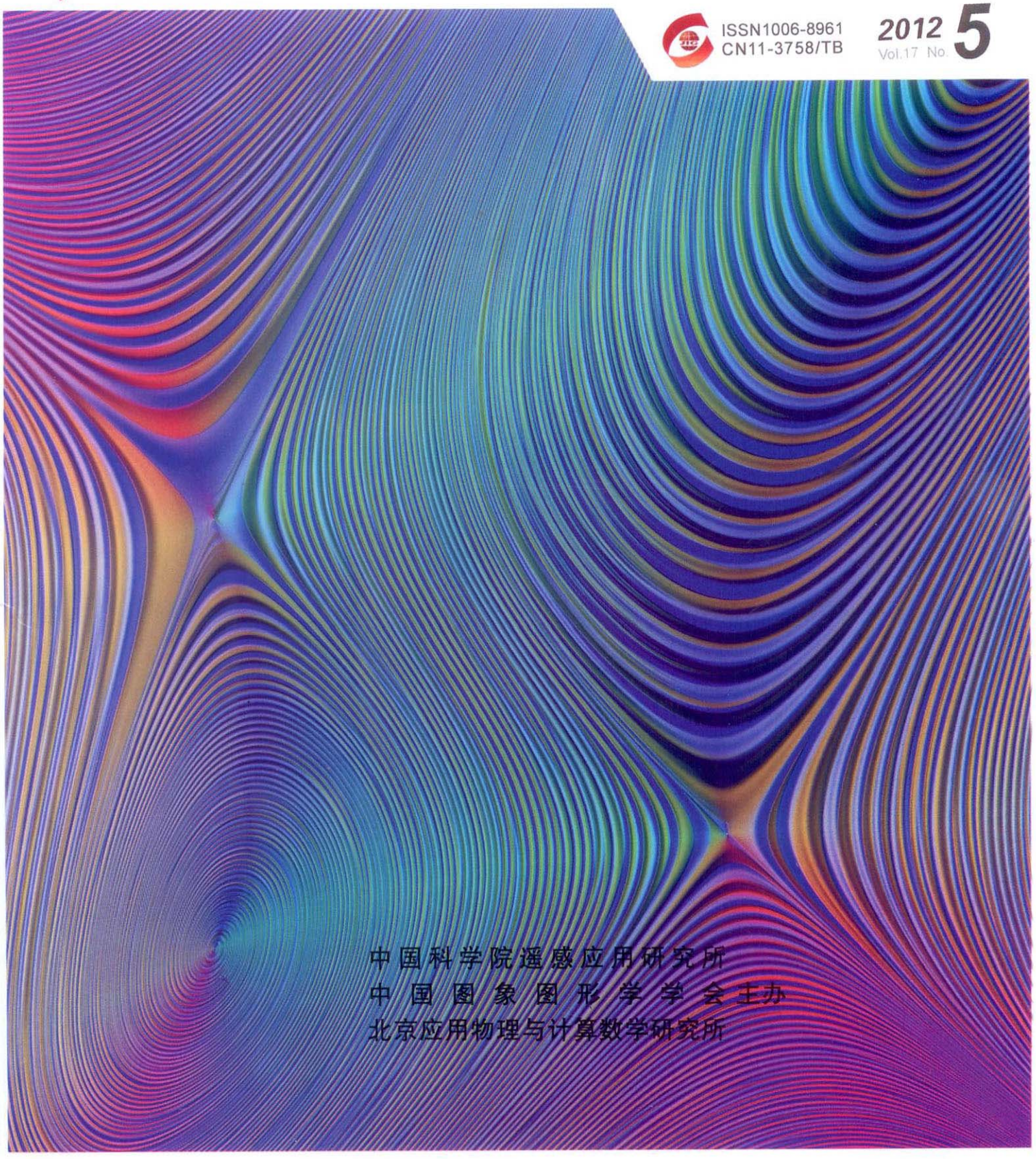
Journal of Image and Graphics

中国图象图形学报

ISSN1006-8961
CN11-3758/TB

2012 5
Vol.17 No.



中国科学院遥感应用研究所
中国图象图形学学会主办
北京应用物理与计算数学研究所

中国精品科技期刊

中国图象图形学报

Zhongguo Tuxiang Tuxing Xuebao

2012 年 5 月　第 17 卷　第 5 期(总第 193 期)

目　次

中国图象图形学报

刊名题字:宋 健　　月刊(1996 年创刊)　　第 17 卷 第 5 期　　2012 年 5 月 16 日出版

主管单位	中国科学院
主　　办	中国科学院遥感应用研究所 中国图象图形学学会 北京应用物理与计算数学研究所
主　　编	李小文
编辑出版	《中国图象图形学报》编辑出版委员会 北京 9718 信箱　邮编 100101 电子信箱:jig@ irsa. ac. cn 电话:010-68407995　010-82614429 网　址:www. cjig. cn
印刷装订	北京北林印刷厂
广告经营许可证	京朝工商广字第 0346 号
总 发 行	北京报刊发行局
订　　购	全国各地邮局
国外发行	中国国际图书贸易总公司 (中国国际书店) (北京 399 信箱　邮编 100044)

Superintended by	Chinese Academy of Sciences
Sponsored by	Institute of Remote Sensing Application, CAS China Society of Image and Graphics Institute of Applied Physics and Computational Mathematics
Chief editor	LI Xiaowen
Editor, Publisher	Editorial and Publishing Board of Journal of Image and Graphics (P. O. Box 9718, Beijing 100101, China) E-mail:jig@ irsa. ac. cn
Distributed by	Beijing Bureau for Distribution of Newspapers and Journals
Domestic	All Local Post Offices in China
Foreign	China International Book Trading Corporation (P. O. Box 399, Beijing 100044, China)
Printed by	Beijing Beilin Printing House

ISSN 1006-8961　CN11-3758/TB　CODE ZTTXFZ　国内邮发代号:82-831　国外发行代号:M1406　国内定价:45.00 元

Journal of Image and Graphics

(**Monthly, Started in 1996**)

Vol. 17 No. 5 May 2012

Contents

中图法分类号: TN309 **文献标志码**: A **文章编号**: 1006-8961(2012)05-0621-07
论文引用格式: 马丽红,吕先明,高小满. 高位有效位概率算术解码的图像密写改进算法[J]. 中国图象图形学报,2012,17(5):621-627

高位有效位概率算术解码的图像密写改进算法

马丽红, 吕先明, 高小满
华南理工大学电子与信息学院,广州 510640

摘 要: 提出一种基于 MSBs(高位有效位)概率算术解码的 DCT(离散余弦变换)域 YASS (yet another steganographic scheme)密写改进算法。为了克服 YASS 算法因量化索引调制(QIM)嵌入特性造成的易攻击缺陷,在 YASS 消息嵌入中用原型信号 MSBs 概率分布约束的算术解码,使消息嵌入流的解码序列具有与原型信号一致的边缘分布,在保持 YASS 算法高随机性嵌入优点的同时,能使密写前后一阶分布直方图之间的差异最小化,有效保证了密写的安全性。实验结果表明,与 YASS 对比,该方法使系数分布直方图的平均变化量更小,其平均失真为 6.3%,相比 YASS 的平均失真 6.8%,减少了 0.5%,改进算法的抗隐写分析能力比后者更强,是一种有效的密写算法。
关键词: 密写;YASS;高位有效位概率;算术解码

Most significant bits probability arithmetic decoding for improved image steganography

Ma Lihong, Lv Xianming, Gao Xiaoman
School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640, China

Abstract: To overcome the attacking-prone drawbacks of quantization index modulation (QIM) in YASS (yet another steganographic scheme), an improved YASS algorithm based on MSBs (most significant bits) arithmetic decoding in DCT domain is proposed. First, a secret sequence is viewed as an arithmetic coding stream and recovered by arithmetic decoding with the MSBs probability of a cover signal distributed, thus the codec reset results in a same marginal distribution between decoding stream and the cover. Then, the decoded bits are reembedded as the convention. Combined with the highly random embedding of YASS, the proposed scheme has a higher security with the first order distribution historgram between the cover and the stego minimized. Experiments demonstrate that the proposed method outperforms YASS both in capability of anti-steg-analysis and the performance of coefficient distribution historgram, which is 6.8% for YASS and 6.3% for the improved one in average. It is an effective steganographic algorithm.
Key words: steganography; yet another steganographic scheme; most significant bits probability; arithmetic decoding

0 引 言

数字密写用于保证信息安全,它在载体中嵌入尽可能多的秘密消息,但嵌入消息越多,原始载体统计特性的破坏越严重,越易被密写分析者觉察。

目前,公认安全性较高的 JPEG 图像密写方法有 F5 算法[1]、OutGuess 算法[2]和基于参数模型的密写算法(MB)[3]。用 Hash 函数实现矩阵编码的 F5 算法,通过改变 1 位 LSB(least significant bit)来

收稿日期:2011-08-16;**修回日期**:2011-11-08
基金项目:国家自然科学基金项目(60972133, 61105010);广东省自然科学基金项目(9351064101000003);广东省能源技术重点实验室项目(2008A060301002)
第一作者简介:马丽红(1965—),女,教授,1999 年于华南理工大学获无线电所通信与电子系统博士学位,主要从事图像视频信号处理、容错编码和数据隐藏、模式识别方面的研究。E-mail: eelhma@scut.edu.cn

实现 k 个信息位的嵌入,使密写信号对载体信号的LSB改动量最小[1],但其缺点是:1)嵌入后零系数增多,统计直方图改变易被识破;2)通过对载密图像的裁剪和再压缩,可使F5密写信号被破解。OutGuess算法利用伪随机序列确定嵌入位置,但需要保留约一半可用系数来修正另一半系数嵌入导致的总体统计偏差[2]。基于模型的密写算法用载体DCT系数MSBs分布来重置解码后的初始载密信号,并修正非零交流(AC)系数的嵌入值以产生最终的载密信号,很难被一阶统计攻击破解[3]。改进的矩阵编码密写算法(MME)在F5的$(1,n,k)$基础上,通过对F5确定的嵌入位置作分解,从几组可选系数中选取一组作嵌入,使可选载密与载体图像间失真最小,达到(t,n,k)的嵌入效率[4]。但是,MME算法密写容量低,且可被密写分析方法破解。经典的裁剪自校正方法,根据载体与载密图像之间的差分分布和可视分块效应来逼近原始统计特性,可破解OutGuess和F5[5-6]。特别是基于DCT特征的盲隐写分析方法,通过设计分类器可有效破解F5、MB、和OutGuess等多种算法[7-8];而基于DCT系数绝对值差异单步转移概率的马尔可夫过程统计特征盲隐写分析方法,针对上述隐写方法也取得了较好的效果[9-10]。文献[11]则结合DCT和马尔可夫特征,通过设计多类分类器获得了更高的检测率。修改的自校准方法同时考虑校准和非校准特征,增加特征维数,进一步扩大了隐写分析范围[12]。但这些方法难以有效破译一种新出现的YASS密写算法。

通过牺牲密写容量获得高安全性的YASS抗盲检测密写算法,其安全策略是使嵌入位置高度随机化,使分析者难以获得好的估计[13]。但受密写容量的限制,YASS选用的嵌入块的承载块不能太大,其密写位置不够随机,因而使嵌入块的起始点可以被一定概率检测;其量化索引调制(QIM,Quantization Index Modulation)嵌入会增加嵌入直方图中对应QIM步长倍数的DCT系数值的个数,减少它值系数的个数,系数嵌入特征因此可被检测出来[14-15]。基于矩阵编码嵌入的改进YASS方法使用(7,4)纠错汉明码较少改动载体系数,提高了嵌入效率和安全性[16]。而根据DCT系数的方差调节设计量化因子的选取,增加了嵌入参数的随机性[17],其秘密消息交互重复嵌入的方式,代替了对秘密消息进行的重复累积(RA)编码以提高数据嵌入率。

为了克服QIM嵌入的缺陷,本文算法中应用DCT AC系数截断分布模型对消息流进行算术解码,使嵌入载体的消息在统计意义上产生与载体系数的一致分布特性,提高密写安全性。

1 YASS及其QIM嵌入的可攻击性

YASS算法利用QIM嵌入的鲁棒性和随机嵌入子块在随机尺寸承载块上的随机起始位置较好地实现了密写的隐秘性,具有一定抗攻击能力,其具体过程可归纳为:

1)秘密消息加工 用RA码对待嵌入的秘密消息编码,得到具有纠错功能的消息流 $\boldsymbol{m}$。

2)承载块和嵌入块选定 将给定的JPEG图像解压到空域,并划分成连续而不重叠的承载块,块大小为 $B\times B$,其中 $B>8$,称之为 B 块(B-block)。在每个 B 块中,根据密钥选取一个 8×8 隐藏子块H-block的起始点,这些子块用来做消息嵌入。

3)嵌入操作 首先对H-block进行2维DCT变换;然后根据自定义的嵌入量化因子 QF_{H} 进行量化,编码后的秘密消息流 $\boldsymbol{m}$ 以QIM的方式嵌入指定的低频AC系数上;最后将嵌入块的系数以量化因子 QF_{H} 反量化并进行2维DCT逆变换,还原为空域信号。

4)载密图像形成 对整幅图像进行JPEG压缩,压缩质量因子为 QF_{α},得到载密图像。

YASS消息提取过程与嵌入过程类似:1)以 QF_{α} 解压载密图像;2)根据密钥提取所有H-block;3)对H-block的2维DCT系数根据 QF_{H} 进行量化,量化系数经QIM量化解密,提取消息流 $\boldsymbol{m}$ 和经RA码判决,获取最原始秘密消息。

YASS算法对载密图像的影响主要来自于QIM嵌入。相比未嵌入的载体量化系数,经过QIM嵌入得到的载体系数会造成异常的局部随机性[18]。YASS算法使用奇量化器量化消息"1"对应的DCT系数,用偶量化器量化消息"0"对应的系数,量化示意图如图1所示,图中 Δ 为量步长。

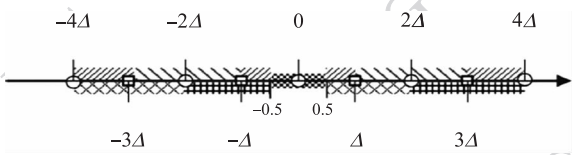


图1 YASS算法中QIM量化示意图[14]

Fig. 1 QIM quantization in YASS algorithm[14]

令未取整的 DCT 系数为 $D_{i,j}$,QIM 嵌入后系数为 $D'_{i,j}$,嵌入消息 $m_{i,j}$,$i,j\in[0,7]$,则有[14]

$$D'_{i,j}=\begin{cases}\mathrm{QIM}(D_{i,j}) & D_{i,j}\notin[-0.5,0.5)\\ D_{i,j} & \text{其他}\end{cases}\tag{1}$$

$$\mathrm{QIM}(D_{i,j})=\begin{cases}2\Delta\left\lfloor\dfrac{D_{i,j}+\Delta}{2\Delta}\right\rfloor & \forall\ m_{i,j}=0\\ 2\Delta\left\lfloor\dfrac{D_{i,j}}{2\Delta}\right\rfloor+\Delta & \forall\ m_{i,j}=1\end{cases}\tag{2}$$

式中,$\lfloor\cdot\rfloor$是下取整运算,Δ 为量化步长。当嵌入消息 $m_{i,j}=0$ 时,$[-\Delta,-0.5)\cup[0.5,\Delta)$区间的系数将量化成 0,$\Delta$ 越大,量化后的系数聚类机会越大,随机性越低,且更多的系数量化为 0。而对于一般的量化操作,系数$\in[-0.5,0.5)$时量化为 0,系数属于$[k-0.5,k+0.5)$时量化为 k,显然与 QIM 量化结果不同。

图 2 为 Lena 图像(1,1)处 AC 系数一般量化与 QIM 量化结果,从图中明显可以看出 QIM 量化造成更多的零系数增加,并且随着量化步长 Δ 增加系数聚类越明显,奇系数值消失,随机性大大降低。由于 QIM 操作使得低频系数本身存在较强的相关性,这必然造成 DCT 系数的块间相关性变弱,这一特征可用于区分载体图像和载密图像,因此密写被识破。

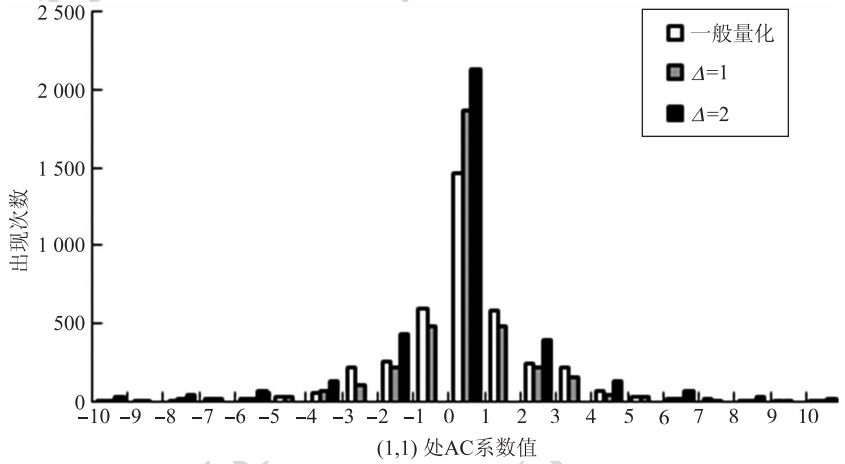


图 2　Lena 图像一般量化与 QIM 量化

Fig. 2　General quantization and QIM quantization

2　基于模型的 YASS 算法

针对 YASS 中 QIM 量化操作造成 DCT 系数统计特性的改变,应用一种基于模型的 YASS 密写方法(MB-YASS)。MB 算法根据载体 DCT 系数低位截断的概率分布来调整嵌入数据,使得嵌入后的系数统计特性最大程度地匹配载体图像的数据分布特性,并且嵌入容量比较大[3]。

设载体信号 $\boldsymbol{X}$ 的概率分布为 $\boldsymbol{P}_x$,将 $\boldsymbol{X}$ 分为两部分截断信号,其中 $\boldsymbol{X}_\alpha$ 是高位信号,$\boldsymbol{X}_\beta$ 是低位信号,$\boldsymbol{X}=(\boldsymbol{X}_\alpha,\boldsymbol{X}_\beta)$。对于嵌入消息 $\boldsymbol{m}$,$\boldsymbol{X}_\alpha$ 保持不变,$\boldsymbol{X}_\beta$ 经消息嵌入后为 $\boldsymbol{X}'_\beta$,得到载密信号 $\boldsymbol{X}'=(\boldsymbol{X}_\alpha,\boldsymbol{X}'_\beta)$。MB 的思想是由 $\boldsymbol{X}_\alpha$ 估计出合适的载体信号概率分布模型 $\boldsymbol{P}'_x$ 来决定 $\boldsymbol{X}_\beta$ 的条件概率分布 $\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$,其条件概率用于约束秘密消息的算术解码,使得解码后的消息流具有与载体信号一致的边缘分布。设算术解码后的消息流概率分布为 $\boldsymbol{P}'_m$,$\boldsymbol{P}'_m$ 需要满足的一致性条件是[3]

$$\boldsymbol{P}'_m=\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha}(\boldsymbol{X}_\beta\mid\boldsymbol{X}_\alpha=x_\alpha)\tag{3}$$

因为 $\boldsymbol{X}$ 与 $\boldsymbol{X}'$的高位信号 $\boldsymbol{X}_\alpha$ 是一样的,故高位信号的概率分布模型 $\boldsymbol{P}'_x$ 和低位信号条件概率分布 $\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$均保持不变,且可用于约束载密信号的低位信号 $\boldsymbol{X}'_\beta$在解码端的算术编码,从而提取秘密消息。

一幅自然图像,其 DCT 变换后的 AC 系数分布可由广义柯西分布的一个特殊形式来描述[3]

$$f(x,p,s)=\frac{p-1}{2s}\left(\left|\frac{x}{s}\right|+1\right)^{-p}\tag{4}$$

式中,x 表示 AC 系数值,p 和 s 分别为位置参数和尺度参数,$p>1$,$s>0$。

用 $h_k^{(i,j)}$ 表示 H-block 中 DCT 系数块第(i,j)AC 位置上值为 k 系数出现的次数,令[3]

$$b_k^{(i,j)}=\begin{cases}h_{2k+1}^{(i,j)}+h_{2k}^{(i,j)} & k<0\\ h_0^{(i,j)} & k=0\\ h_{2k-1}^{(i,j)}+h_{2k}^{(i,j)} & k>0\end{cases}\tag{5}$$

定义 $\boldsymbol{h}^{(i,j)}$ 为高精度直方图分布，$\boldsymbol{b}^{(i,j)}$ 为低精度直方图分布，嵌入消息前后 $\boldsymbol{b}^{(i,j)}$ 不变，所以 $\boldsymbol{b}^{(i,j)}$ 是载体信号 $\boldsymbol{X}$ 中的 $\boldsymbol{X}_\alpha$，$\boldsymbol{h}^{(i,j)}$ 是 $\boldsymbol{X}_\beta$。$\boldsymbol{X}_\alpha$ 的概率分布 $\boldsymbol{P}'_x$ 由柯西分布(式(4))拟合得到，而 $\boldsymbol{X}_\beta$ 在当前 $\boldsymbol{X}_\alpha$ 下的条件分布 $\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$ 可由累积密度函数获得[3]

$$P_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}=\begin{cases}\dfrac{1}{2}\left(1+\left|\dfrac{x}{s}\right|\right)^{1-p} & x\leqslant 0\\ 1-\dfrac{1}{2}\left(1+\left|\dfrac{x}{s}\right|\right)^{1-p} & x\geqslant 0\end{cases} \tag{6}$$

根据 $P_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$ 对秘密消息进行算术解码后，解码流再改写到 H-block 非零 AC 系数的低位位置上可获得载密对象 $\boldsymbol{X}'=(\boldsymbol{X}_\alpha,\boldsymbol{X}'_\beta)$，其中 $\boldsymbol{X}_\alpha$ 分布与载体对象是一致的。

在改进的 YASS 算法中，用 MB 嵌入替代 QIM。与 QIM 类似，MB 算法不在 0 系数位置上嵌入消息[3]，即当 $D_{i,j}\in[-0.5,0.5)$ 时，系数保持不变，其他系数则要经量化再做 MB 嵌入，具体的 MB 消息嵌入机制如图 3 所示。

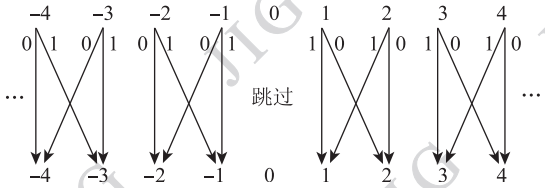


图 3 MB 消息嵌入机制

Fig. 3 Embedding mechanism of MB

从图 3 可以看出，MB 嵌入使得系数的改变范围局限于两个相邻的系数中，例如系数值 1 和 2 经 MB 嵌入后仍然为 1 或 2，而不会跳变到其他位置，不会造成分布直方图中 0 系数的增加；而 QIM 受量化参数 Δ 影响，Δ 越大，系数聚类机会越大，越容易破坏 DCT 系数的块间相关性，且会造成分布直方图中 0 系数的增加，使隐写更容易被识破。另外，由于 MB 算法消息嵌入前后维持低精度分布 $b^{(i,j)}$ 不变，系数统计分布收敛于广义柯西分布，因为这能够很好的保持载体和载密图像的系数分布。

MB-YASS 算法消息嵌入流程如图 4 所示。

1)由原始 YASS 算法获取所有 H-block，即载体 H-block。

2)计算 H-block 经 Zigzag 扫描后的前 19 个低频 AC 系数位置低精度直方图，并估计每个 $\boldsymbol{P}'_x$ 分布。

3)根据 $\boldsymbol{P}'_x$ 计算高精度直方图的概率分布 $\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$。

4)根据 $\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$ 对 RA 编码后的秘密消息进行算术解码后再改写到载体相应 AC 系数低位位置上得到载密 H-block，然后反量化、DCT 逆变换、JPEG 压缩、重复原始 YASS 算法步骤。

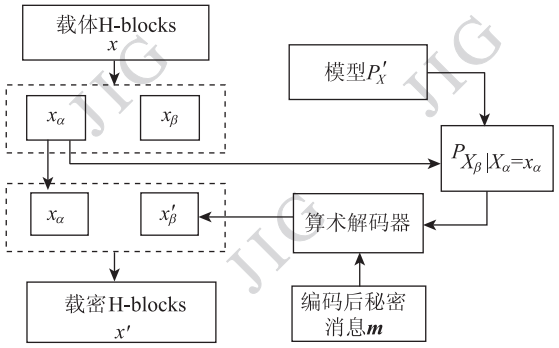


图 4 MB-YASS 算法消息嵌入流程

Fig. 4 Message embedding process of MB-YASS algorithm

消息提取时，将载密 H-block 的非零 AC 系数的低位数据根据 $\boldsymbol{P}_{\boldsymbol{X}_\beta|\boldsymbol{X}_\alpha=x_\alpha}$ 进行算术编码，获取秘密消息，消息提取算法流程如图 5 所示。

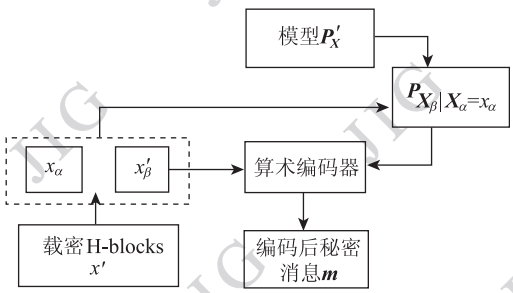


图 5 MB-YASS 算法消息提取流程

Fig. 5 Message extraction process of MB-YASS algorithm

3 实验结果

为验证 MB-YASS 的有效性，与 YASS 进行对比实验，验证指标包括：1)系数分布直方图保持能力；2)嵌入容量对比；3)抗攻击性能分析；4)抗隐写分析能力比较。为了使消息比特序列均匀分布，嵌入前先对其混沌置乱，实验样本图像包括标准测试图像库的 16 幅 JPEG 灰度图像，NRCS 图像库中的 800 幅未压缩彩色 JPEG 图像以及 Canon 相机拍摄的 800 幅 JPEG 图像，选取 H-block 经 Zigzag 扫描后的前 19 个低频 AC 系数位置作为密写位置，QIM 量化步长 $\Delta=1$，载体和载密图像最终均以 $QF_\alpha=75$ 压缩。

3.1　系数分布直方图保持能力

图 6(a)(b)给出了 Lena 和 Baboon 密写前后的(1,1)和(2,2)频率位置处系数分布直方图,横坐标为 AC 系数值(仅显示范围[-10,10]),纵坐标为系数的出现次数。图 6(c)给出了 16 幅标准测试图像经 Zigzag 扫描后的前 19 个系数位置的平均直方图失真,横坐标为图像的序号。可以看出:

1)系数分布直方图中零系数个数的变化:嵌入后 MB-YASS 分别使零系数个数变化了 2.09%(图 6(a))和 1.84%(图 6(b)),而 YASS 相应地变化了 3.37%(图 6(a))和 2.78%(图 6(b)),明显高于 MB-YASS,这是因为 MB 没有在 H-block 零系数上做嵌入。

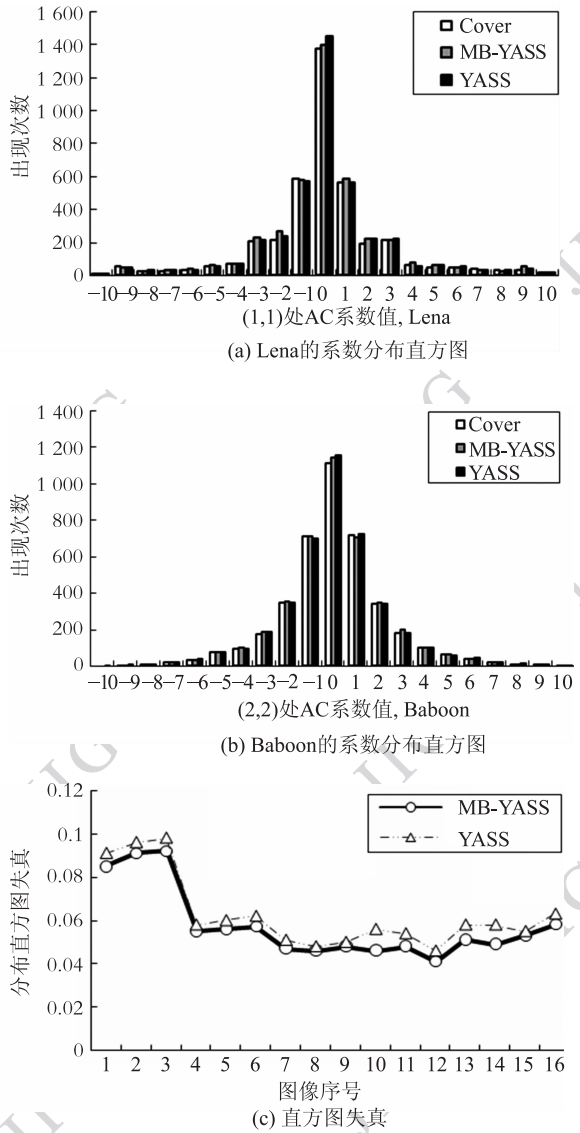


图 6　两种 YASS 算法系数分布直方图和直方图失真比较

Fig. 6　Comparison of coefficient distribution histogram and histogram distortion between two YASS algorithms

2)系数分布直方图中非零系数个数的变化:MB-YASS 使非零系数个数的平均变化为 7.1%(图 6(a))和 7.6%(图 6(b)),低于 YASS(7.3% 和7.9%)。

3)MB-YASS 的平均直方图失真为 0.062(图 6(c)),低于 YASS 的 0.068。原因是 MB 嵌入保持了载体的概率分布,使载体和载密图像之间直方图失真较小。

3.2　嵌入容量对比

表 1 为两种 YASS 算法在不同 B 块大小下的嵌入容量对比。这里的嵌入容量定义为所有 H-block 经 Zigzag 扫描后前 19 个低频系数位置嵌入的总消息比特数之和。可以看出 MB-YASS 具有较大的消息嵌入容量,但略低于 YASS。

表 1　两种 YASS 算法嵌入容量

Table 1　Embedding capacity of two YASS algorithms

B 块大小	Lena		Baboon	
	YASS	MB-YASS	YASS	MB-YASS
10	14 408	11 941	30 934	27 358
15	6 371	4 850	13 855	12 223
20	3 052	2 711	7 432	6 591

3.3　抗攻击性能分析

攻击测试包括 χ^2 分析和裁剪分析,测试样本为标准测试图像库的 16 幅 JPEG 图像,下面比较两种 YASS 算法的抗攻击能力。

1)χ^2 分析。对待检测的图像,χ^2 检验分析可有效检测密写造成载体 DCT 系数对值(pair values)的变化,其思想是将密写图像的理论概率分布与可能被修改过的载体的样本分布进行比较,从而找出差异[19]。对于 χ^2 分析,定义统计量

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(P(X = 2i) - P(Y = 2i))^2}{P(Y = 2i)} \quad (7)$$

式中,X 为载密图像系数实际值,Y 为载密图像系数理论值,取 AC 系数对(1,2)、(3,4)、(5,6)、(-1,-2)、(-3,-4)和(-5,-6)作统计,因此样本数 $k=6$。我们作以下假设检验:如果统计量大于临界值 11.071,那么图像怀疑被密写的概率小于 0.05。图 7(a)给出了两种算法密写后 AC 系数 χ^2 分析的平均统计量,两种算法的统计量都在临界线之上,因此均能抗 χ^2 分析。

2)裁剪分析。裁剪自校正原理:解压到空域的载密图像自左上角裁剪掉 4 行 4 列之后再以相同的量化表压缩,压缩后的裁剪载密图像 DCT 系数统计

特性能够很好的逼近载体图像的 DCT 系数统计特性[5]。因此,可通过载体图像和载密图像裁剪分析的统计差异来检验密写算法的安全性。图 7(b)给出了两种算法裁剪分析的一阶直方图失真,图中的实线代表裁剪后载体图像与原始载体图像之间的直方图失真 ρ',而虚线代表裁剪后载密图像与原始载密图像之间的直方图失真 r^i。ρ'(或 r^i)越小,裁剪估计越准确;r^i 越接近于 ρ',载密图像被认为载体图像的概率越大。由图 7(b)可知,MB-YASS 和 YASS 的 r^i 分别为 0.083 和 0.082,均与 ρ'(0.081)相当。因此,MB-YASS 和 YASS 都能抗裁剪分析。

3.4 抗隐写分析能力比较

与盲隐写分析方法类似[7-12],本文隐写分析结果以检测概率 P_{detect} 来表示,通过支持向量机(SVM)来训练载体和载密图像,实现两类分类。本节测试样本选自 NRCS 图像库中的 800 幅未压缩的彩色图像和 Canon 相机拍摄的 800 幅 JPEG 图像,取其中心的 512 × 512 部分,然后以 $QF_\alpha = 75$ 压缩,作为载体图像。从两图像库中随机各取 800 幅载体图像及其对应载密图像用于训练,余下的 800 幅载体及其对应载密图像用于测试。

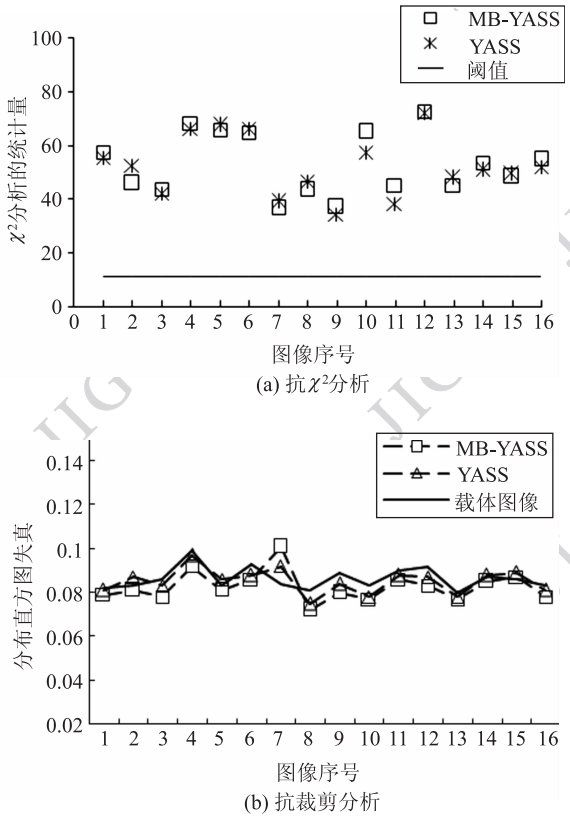


图 7 两种算法的抗攻击能力比较

Fig. 7 Comparison of anti-attack capability between two algorithms

选择文献[11-12]中的隐写特征来验证算法的安全性,即 Pevn′y 等人 274 维校准的 DCT 和 Markov 特征(PF-274)[11]以及 Kodovsk ý等人修改的 548 维校准特征(KF-548)[12]。令 $\boldsymbol{X}_0$ 和 $\boldsymbol{X}_1$ 分别表示已知的载体图像(类"0")和载密图像(类"1"),$\boldsymbol{Y}_0$ 和 $\boldsymbol{Y}_1$ 为 SVM 分类出的载体图像(类"0")和载密图像(类"1"),当 $P(X_0) = P(X_1) = 1/2$ 时,检测概率 P_{detect} 定义为[16]

$$P_{\text{detect}} = 1 - P_{\text{error}} \tag{8}$$

$$P_{\text{error}} = P(\boldsymbol{X}_0)P(\boldsymbol{Y}_1 \mid \boldsymbol{X}_0) + P(\boldsymbol{X}_1)P(\boldsymbol{Y}_0 \mid \boldsymbol{X}_1) = \frac{1}{2}P_{\text{FA}} + \frac{1}{2}P_{\text{miss}}$$

式中,$P_{\text{FA}} = P(\boldsymbol{Y}_1 \mid \boldsymbol{X}_0)$ 和 $P_{\text{miss}} = P(\boldsymbol{Y}_0 \mid \boldsymbol{X}_1)$ 分别表示虚警和错失的概率。当载体和载密图像数量相等时 $\left(P(\boldsymbol{X}_0) = P(\boldsymbol{X}_1) = \frac{1}{2}\right)$,$P_{\text{detect}}$ 接近 0.5,密写则不能检测,P_{detect} 越接近 1 则表示密写被识破的概率越接近 1。

表 2—3 分别为两种 YASS 算法在不同 QF_{H} 参数下的被检测概率对比。实验结果表明,当 $QF_{\text{H}} = 55$ 时,相同 B 块大小下 MB-YASS 算法检测概率均低于 YASS(表 2),即算法安全性高于 YASS,随着 B 块大小增加到 16,两种 YASS 算法被检测的概率均接近 0.5,这时两种密写算法不能被检测;当 $QF_{\text{H}} = 75$ 时,两种算法抗隐写性能相当,均能抵抗上述两种隐写特征的分析(表 3)。因此可以看出,MB-YASS 算法是一种有效的图像密写算法。

表 2 两种 YASS 算法检测概率比较,$QF_{\text{H}} = 55$

Table 2 Comparison of detect probability between two YASS algorithms, $QF_{\text{H}} = 55$

密写算法	B = 9		B = 11		B = 13		B = 16		B = 20	
	PF-274	KF-548	PF-274	KF-548	PF-274	KF-548	PF-274	KF-548	PF-274	KF-548
YASS	0.78	0.85	0.73	0.79	0.66	0.68	0.53	0.54	0.53	0.52
MB-YASS	0.74	0.82	0.68	0.76	0.64	0.65	0.52	0.55	0.52	0.52

表 3　两种 YASS 算法检测概率比较,$QF_H=75$

Table 3　Comparison of detect probability between two YASS algorithms, $QF_H=75$

密写算法	B=9		B=11		B=13		B=16		B=20	
	PF-274	KF-548	PF-274	KF-548	PF-274	KF-548	PF-274	KF-548	PF-274	KF-548
YASS	0.57	0.56	0.54	0.54	0.54	0.56	0.54	0.54	0.53	0.52
MB-YASS	0.57	0.58	0.54	0.53	0.56	0.55	0.52	0.54	0.52	0.53

4　结　论

提出一种基于 MSBs 概率算术解码的高安全性 JPEG 图像 YASS 密写算法,在消息嵌入过程中引入基于 MSBs 概率算术解码方法,该方法通过计算载体 MSBs 概率分布,算术解码秘密消息,解码后的消息序列嵌入载体非零 AC 系数低位位置上,克服了 QIM 嵌入造成的 0 系数的增加,减少了载体和载密图像系数直方图分布的差异,提高了 YASS 算法的安全性。

参考文献(References)

[1] Westfeld A. F5-A steganographic algorithm[C]//Proceedings of the 4th International Workshop on Information Hiding. Berlin: Springer-Verlag, 2001: 289-302.

[2] Provos N. OutGuess: Steganography detection with Stegdetect [EB/OL]. (2008-07-12) [2011-08-17]. http://www.outguess.org.

[3] Sallee P. Model-based methods for steganography and steganalysis[J]. International Journal of Image and Graphics, Image Data Hiding, 2005, 5(1):167-189.

[4] Kim Y, Duric Z. Modified matrix encoding technique for minimal distortion steganography [C]//Proceedings of the 8th International Workshop on Information Hiding. Berlin: Springer-Verlag, 2007: 314-327.

[5] Fridrich J, Golian M, Hogea D. Steganalysis of JPEG images: Breaking the F5 algorithm [C]// Proceedings of the 5th Information Workshop on Hiding Workshop. Berlin: Springer-Verlag, 2002: 310-323.

[6] Fridrich J, Golian M. Attacking the OutGuess [C]// Proceedings of the ACM Workshop on Multimedia and Security. New York: ACM, 2002: 256-262.

[7] Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes[C]// Proceedings of the 6th International Workshop on Information Hiding. Berlin: Springer-Verlag, 2004: 67-81.

[8] Fridrich J, Pevn'y T. Multi-class blind steganalysis for JPEG images[C]//Proceedings of the International Society for Optical Engineering. Bellingham, Washington: SPIE, 2006:257-269.

[9] Chen C H, Shi Y Q. JPEG image steganalysis utilizing both intrablock and interblock correlations[C]//Proceedings of the IEEE International Symposium on Circuits and System. Seattle: IEEE, 2008: 3029-3032.

[10] Davidson J, Jalan J. Steganalysis using partially ordered markov models[C]//Proceedings of the 12th International Conference on Information Hiding. Berlin: Springer-Verlag, 2010:118-132.

[11] Pevn'y T, Fridrich J. Merging markov and DCT features for multi-class JPEG steganalysis [C]//Proceedings of the International Society for Optical Engineering. Bellingham, Washington: SPIE, 2007:1-13.

[12] Kodovsky J, Fridrich J. Calibration revisited [C]//Proceedings of the 11th ACM Workshop on Multimedia and Security. New York: ACM, 2009:63-74.

[13] Solanki K, Sarkar A. YASS: Yet another steganographic scheme that resists blind steganalysis [C]//Proceedings of the 9th International Workshop on Information Hiding. Berlin: Springer-Verlag, 2007:16-31.

[14] Li Bi, Huang J W, Shi Y Q. Steganalysis of YASS[J]. IEEE Transactions on Information Forensics and Security, 2009, 4(3):369-382.

[15] Yu X Y, Babaguchi N. Breaking the YASS algorithm via pixel and DCT coefficients analysis[C]//Proceedings of the 19th International Conference on Pattern Recognition. Tampa, Florida: IEEE, 2008: 1-4.

[16] Sarkar A, Madhow U, Manjunath B S. Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2):225-239.

[17] Sarkar A, Solanki K, Manjunath B S. Further study on YASS: Steganography based on randomized embedding to resist blind steganalysis[C]// Proceedings of the International Society for Optical Engineering. Bellingham, Washington: SPIE, 2008: 16-31.

[18] Malik H. Steganalysis of QIM steganography using irregularity measure [C]//Proceedings of the 10th ACM Workshop on Multimedia and Security. New York: ACM 2008: 149-158.

[19] Westfeld A, Pfitzmann A. Attacks on steganographic system [C]//Proceedings of the 3rd International Workshop on Information Hiding. Berlin: Springer-Verlag, 2000:61-76.