第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0140—04 文献标识码：A 中图分类号：TP391

一种新的 JPEG 图像二次压缩检测算法

韩晓东，平西建，张 涛
(解放军信息工程大学信息科学系，郑州 450002)

摘 要：针对隐写分析中 JPEG 图像二次压缩的检测问题，提出一种新的压缩检测算法。通过对 JPEG 一次压缩和二次压缩后的绝对值直方图进行比较，发现直流与交流系数差分绝对值、交流与交流系数差分绝对值在二次压缩后有明显变化。在此基础上提取特征，采用 SVM 进行分类。实验结果表明，在虚警率小于 5%的情况下，该算法检测性能优于 Pevny T 和 Fridrich J 提出的算法(IEEE Trans. on Information Forensics and Security, 2007, No.2)。

关键词：隐写分析；JPEG 图像；质量因子；二次压缩

New Detection Algorithm of Double Compression in JPEG Image

HAN Xiao-dong, PING Xi-jian, ZHANG Tao
(Department of Information Science, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】This paper proposes a new algorithm for detection of double compression in JPEG image for applications in steganalysis, which based on the analysis of the influences on absolute histogram brought about by the double compression. It compares the histograms of single-compressed and double-compressed images and finds that both the absolute differences of DC and AC coefficients and the absolute differences of AC and AC coefficients change obviously after double compression. Support Vector Machine(SVM) classifiers are trained to detect an image whether double-compressed or not. Experimental results show that the proposed method is better than the algorithm proposed by Pevny T and Fridrich J(IEEE Trans. on Information Forensics and Security, 2007, No.2) while the false positive alarm is controlled under 5%.

【Key words】steganalysis; JPEG image; quality factor; double compression

1 概述

信息隐藏(stegonagraph)技术是一种新的信息安全技术，隐写分析(steganalysis)技术是其逆问题。JPEG 图像作为目前 Internet 上广为流行的一种图像格式，以其为载体的经典隐写算法不断涌现，如 JSTEG[1], OUTGUESS[2], F5[3], MB[4]等。同时还出现了许多隐写分析算法。JSTEG 算法由于使用简单的替换技术，导致 DCT 系数直方图中相邻系数出现频次趋于一致。文献[5]设计一种快速 JSTEG 检测算法，对顺序和随机间隔 JSTEG 嵌入率实现了较好的估计。针对 OUTGUESS 和 F5 算法，文献[6-7]将待检测图像解压缩后裁减左 4 行上 4 列再重新压缩得到载体图像的估计，在此基础上对这 2 种隐写算法成功地进行了隐写分析。除了上述这些专用算法以外，也有一些盲隐写分析算法对上述这些算法进行检测。如文献[8]在分析 DCT 系数在嵌入前后统计变化的基础上，提取了 23 维特征并通过裁减方法估计载体图像进行校准，采用 Fisher 线型分类器进行训练和分类，对以 JPEG 图像为载体的隐写算法有很好的检测效果。

分析结果表明，文献[6-8]中提出的隐写分析算法存在一个共同问题：假设待检测图像只经过一次 JPEG 压缩，使用裁剪重压缩方法估计载体图像，而由文献[2-3]中 F5 和 OUTGUESS 算法的嵌入原理可知，在隐写过程中先将载体图像解压缩后再进行重压缩(F5 默认质量因子是 80，OUTGUESS 是 75)，然后进行秘密信息的嵌入。如果在嵌入秘密信息前进行重压缩所用的质量因子与载体图像的质量因子不同时，则嵌密图像为二次压缩图像。文献[6]指出，二次 JPEG 压缩图像与一次 JPEG 压缩图像的 DCT 系数统计特性是明显不同的，忽视了二次压缩的影响可能导致隐写分析产生完全错误的结论。因此，在进行隐写分析前判断 JPEG 图像是否经过二次压缩有非常重要的意义。

文献[6]提出了检测 JPEG 图像是否经过二次压缩的方法，但都是针对载体图像进行的。文献[9]在分析 JPEG 图像二次压缩对 DCT 系数统计产生影响的基础上，提取 144 维特征并使用 SVM 进行训练分类，能够有效检测载体和载密 JPEG 图像是否经过二次压缩。但上述算法只对 JPEG 图像中交流系数在二次压缩过程中产生的变化进行分析，并未考虑直流系数的变化以及直流与交流系数差分的变化。

本文对直流和交流系数差分绝对值、交流和交流系数差分绝对值在二次压缩过程中的统计变化进行分析，并在此基础上提出一种新的图像二次压缩检测算法。

2 JPEG 图像的一次压缩和二次压缩

JPEG 压缩是将原始图像进行 8×8 分块后对每一块进行 DCT 变换，并将变换后的系数按照标准量化表进行量化。量化后的系数按低频到高频的 Z 扫描方式排列。其中，位置(1,1)表示直流系数，代表了 8×8 分块的像素平均值，其余位置表示在 Z 扫描方式下频率由低到高的交流系数。需要说明的是，

基金项目：国家自然科学基金资助项目(60473022)
作者简介：韩晓东(1982－)，男，硕士研究生，主研方向：图像处理，信息隐藏；平西建，教授、博士生导师；张 涛，副教授、博士
收稿日期：2009-07-20 **E-mail：**hanxiaodong100@yahoo.com.cn

标准量化表是一组以质量因{1,2,…,100}标识的量化表组。

设 Q_1 和 Q_2 分别表示一次和二次压缩的质量因子。原始图像(如 TIFF 和 BMP 格式)用质量因子 Q_1 一次压缩后，8×8 分块中交流 DCT 系数的分布服从广义高斯分布。

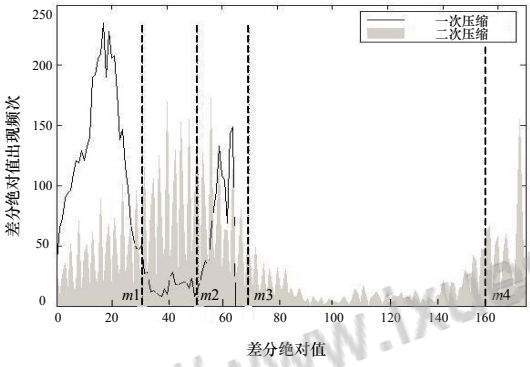
若将其解压缩到空域后再用 Q_2 进行二次压缩，当 $Q_1 \neq Q_2$ 时，称图像经过二次 JPEG 压缩。文献[9]中指出，此时 8×8 分块中交流 DCT 系数的分布不再满足广义高斯分布，而是具有一些很明显的特征：零值和双峰现象。

3 基于系数差分绝对值差异的二次压缩检测算法

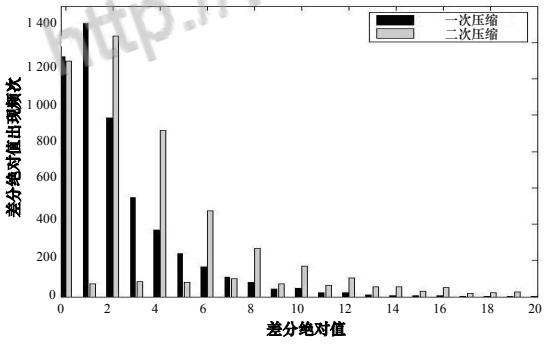
文献[6, 9]提出的算法虽然有一定的检测效果，但只考虑到二次 JPEG 压缩过程对交流系数的改变，并未考虑直流系数、直流与交流系数差分值在二次量化过程中的变化。

3.1 DCT 系数差分绝对值直方图

设 JPEG 图像总的分块数为 l；k 表示第 k 个分块，$\left|DA_{i,j}^{k}\right|$ 和 $\left|AA_{i,j}^{k}\right|$ 分别表示直流与位置(i,j)交流系数的差分绝对值、位置(i, j)的交流系数与 Z 扫描方式下其后一个位置交流系数的差分绝对值。图 1(a)为直流位置(1, 1)与交流位置(1, 2)的 DCT 系数差分绝对值直方图。图 1(b)为 Y 分量中，频率位置(1, 2)与(2,1)处交流 DCT 系数的差分绝对值直方图。



(a)直流与交流系数差分绝对值直方图



(b)交流与交流系数差分绝对值直方图

图 1　系数差分绝对值直方图

图 1(a)为原始 TIFF 格式图像先用质量因子 50 压缩后，再用 F5 算法以默认质量因子 80 重压缩后嵌入 25%秘密信息后的 $\left|DA_{1,2}^{k}\right|$ 直方图比较)；图 1(b)为原始 TIFF 格式图像先后采用 Q_1=50, Q_2=80 二次 JPEG 压缩后 Z 扫描顺序下 $\left|AA_{1,2}^{k}\right|$ 直方图比较。可以发现，一次压缩和二次压缩前后 $\left|DA_{1,2}^{k}\right|$, $\left|AA_{1,2}^{k}\right|$ 直方图有明显不同。

分析原因，不同质量因子对应的量化表中直流和交流位置对应的量化步长是不同的。随着质量因子的增大，量化步长逐渐减小。表 1 列出了质量因子 50 和 80 对应的量化表中 Z 扫描方式下直流与前 5 个交流位置的量化步长。可以发现，量化步长 $Q_{50}^{i,j}$ 和 $Q_{80}^{i,j}$ 有明显差异，其中，直流位置量化步长差异最大。

表 1　直流与交流位置的量化步长

位置	Q=50	Q=80
0	16	6
1	11	4
2	12	5
3	14	6
4	12	5
5	10	4

设 $d_{i,j}$ 表示 JPEG 图像中 8×8 分块的系数，由以上分析可知 $Q^{i,j}$ 的差异导致了 $d_{i,j}$ 在采用不同质量因子量化时的明显差异，其统计规律相应的也发生改变，如图 2 所示。

0	1	5		56	0	1		149	0	2		149	0	2
2	4			-1	0	0		-2	1	0		-2	0	0
3				0	0	0		0	0	0		0	0	0

(a)位置　(b)Q_1=50 压缩　(c)Q_1=80 压缩　(d)二次压缩

图 2　不同位置的系数在不同量化时的系数值

图 2(a)中位置 0 表示直流，其他位置为 Z 扫描顺序下的交流。图 2(b)中一幅原始 TIFF 图像仅用 Q_1=50 压缩时，直流和交流步长都较大，故量化后的直流系数值较小，交流系数值多为 0 或 1(为便于分析，这里采用绝对值)。图 2(c)中仅用 Q_1=80 压缩时，直流和交流步长相对较小，故量化后的直流系数值很大，交流系数非零值增多、增大。图 2(d)中先后用 Q_1=50, Q_1=80 二次压缩时，直流和交流系数相比 Q_1=50 一次量化后改变明显。相应地，直流与交流系数的差分、交流与交流系数的差分也发生了明显的变化。

二次 JPEG 压缩图像不仅可以由原始图像先后采用不同的质量因子二次压缩形成，还可以由原始图像一次 JPEG 压缩后再使用隐写算法生成。如前所述，F5 和 OUTGUESS 算法在隐写过程中先将载体 JPEG 图像解压到空域再进行重压缩，然后进行秘密信息的嵌入。而这 2 种嵌入算法均在 8×8 分块中的交流系数进行嵌入而直流系数不做改动，改变了交流系数的统计特性，使二次 JPEG 压缩载密图像的检测更加困难。因此，本文使用直流与交流系数的差分绝对值、交流与交流系数的差分绝对值来分别衡量由隐写过程中二次 JPEG 压缩、载体图像直接二次 JPEG 压缩所引起的 DCT 系数统计规律变化。

3.2 特征的提取

原始图像在一次 JPEG 压缩的过程中，若质量因子很大，则量化步长很小，低频位置量化系数有较多的非零值，统计意义明显。而一般情况下量化后的中高频系数大多为 0 统计意义不明显。权衡 2 个方面以及考虑到降低运算复杂度，对 9 个低频位置 L={(1, 2),(2, 1),(3, 1),(2, 2),(1, 3),(1, 4),(2, 3), (3, 2), (4, 1)}的 2 个差分绝对值直方图分别进行统计。设 $\left|DA_{i,j}^{k}\right|$ 和 $\left|AA_{i,j}^{k}\right|$ 出现频次分别为 $DAH_{i,j}(m)$ 和 $AAH_{i,j}(m)$，则有:

$$DAH_{i,j}(m)=\sum_{k=0}^{l}\delta\left(\left|DA_{i,j}^{k}\right|-m\right) \tag{1}$$

$$AAH_{i,j}(m)=\sum_{k=0}^{l}\delta\left(\left|AA_{i,j}^{k}\right|-m\right) \tag{2}$$

其中，$(i,j)\in L$，$\delta(x)=\begin{cases}1 & x=0\\ 0 & \text{else}\end{cases}$，令

$$DA_{i,j}=\sum_{m=0}^{160}DAH_{i,j}(m) \tag{3}$$

$$AA_{i,j}=\sum_{m=0}^{15}AAH_{i,j}(m) \tag{4}$$

从图 1(a)可知，在统计直流与交流系数差分绝对值过程

中，计算每一个差分绝对值的频次差异的计算量较大，因此，划分 $m1=30$, $m2=50$, $m3=70$, $m4=160$ 几个区间分别加以考虑：

$$\begin{cases} DA_1=\sum\limits_{m=0}^{m1-1}DAH_{i,j}(m), DA_2=\sum\limits_{m1}^{m2-1}DAH_{i,j}(m) \\ DA_3=\sum\limits_{m2}^{m3-1}DAH_{i,j}(m), DA_4=\sum\limits_{m3}^{m4}DAH_{i,j}(m) \end{cases} \tag{5}$$

则得到反映直流与交流系数差分差异的特征：

$$X=\left\{\frac{1}{DA_{i,j}}(DA_1,DA_2,DA_3,DA_4),\ (i,j)\in L\right\} \tag{6}$$

通过比较发现，对交流与交流系数差分绝对值出现的频次进行累加，能更有效地反映二次压缩前后交流系数差分绝对值的差异程度：

$$AA_m=\sum_{k=0}^{m}AAH_{i,j}(k) \tag{7}$$

则得到反映交流与交流系数差分差异的特征：

$$Y=\left\{\frac{1}{AA_{i,j}}(AA_0,AA_1,\cdots,AA_{14}),\ (i,j)\in L\right\} \tag{8}$$

对于待检测 JPEG 图像，按式(6)、式(8)得到 9 个位置共(15+4)×9=171 个特征后，运用模式识别的方法判断待检测 JPEG 图像是否经过二次压缩。

3.3 分类器的设计

支持向量机(Support Vector Machine, SVM)是模式识别中常用的一种分类器，对样本数量和质量依赖较小，可以用来解决二分类问题。因此，在本文算法中使用 SVM 进行分类识别。

4 实验仿真

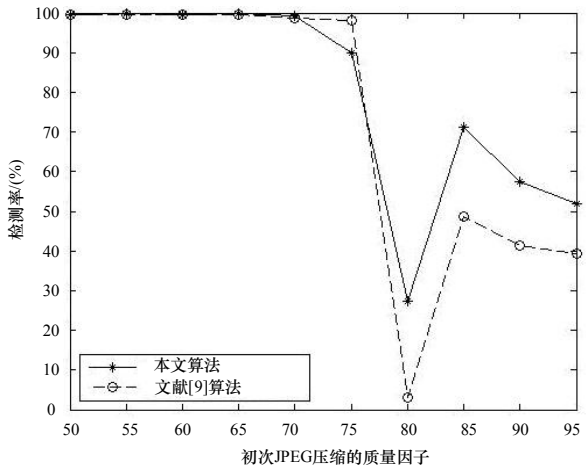
实验从 USDA NRCS Photo Gallery(http://Photogallery.nrcs.usda.gov)中下载 3 000 张 TIFF 格式的原始图像，先将其通过下采样处理为 700×500 的灰度图像。这些图像中的 1 800 张用来生成训练图像，剩余的 1 200 张用来生成测试图像。首先以质量因子 Q=(50, 55, 60, 65, 70, 75, 80, 85, 90, 95)进行一次 JPEG 压缩生成一次压缩载体图像，再以质量因子 80(F5 算法默认质量因子)进行第 2 次 JPEG 压缩生成载体二次 JPEG 压缩图像。为了对载密图像是否经过 JPEG 二次压缩进行检测，对原始 TIFF 格式图像使用 F5 算法分别以质量因子 Q=(50, 55, 60, 65, 70, 75, 80, 85, 90, 95)生成不同嵌入率 25%, 50%, 100%下的一次压缩载密图像。然后对一次压缩载体图像使用 F5 算法采用默认质量因子 80 分别以嵌入率 25%, 50%, 100%生成不同嵌入率下的二次压缩载密图像。这样就生成了总共 $10\times(4+4)\times(1\,800+1\,200)=240\,000$ 张 JPEG 图像的实验库。SVM 类型为 C-SVC，核函数选择为径向基函数内核。实验仿真在 Pentium(R) 4 双核 CPU3.00 GHz，内存 512 MB 的电脑上进行。为了对算法性能进行比较，本文在相同的图像库上对 Pevny T 和 Fridrich J 提出的的算法[9]进行仿真。

对于 Q 中的每一个质量因子，训练图像的选取如表 2 所示。其中不同嵌入率下选取的 600 幅图像均为随机选取，这样共有 72 000 张图像参加训练。

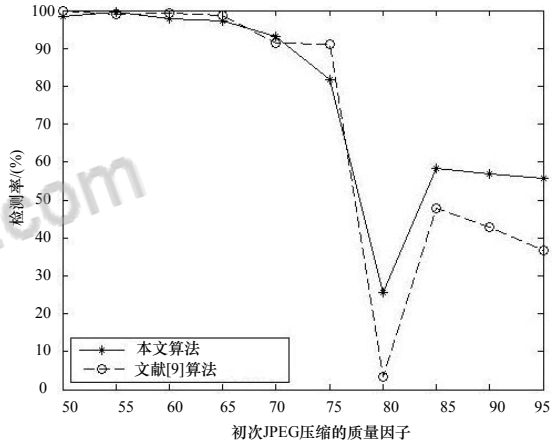
表 2 训练图像的选取 幅

	嵌入率=25%	嵌入率=50%	嵌入率=100%
一次压缩	600	600	600
二次压缩	600	600	600

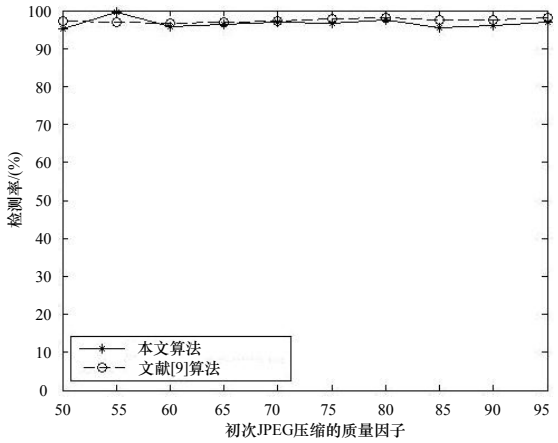
训练完成后，为了不失一般性，对应不同的一次压缩质量因子 Q，随机选取二次 JPEG 压缩载体图像 1 200 张，不同嵌入率下二次 JPEG 压缩载密图像各 400 张。对载体图像和混合载密图像分别进行检测，用以比较 2 种算法的虚警率。结果如图 3 所示。其中，图 3(b)为不同嵌入率下的混合二次 JPEG 压缩载密图像检测结果；图 3(c)为一次 JPEG 压缩载体图像 1 200 张与不同嵌入率下的一次 JPEG 压缩载密图像各 400 张混合时的检测结果。



(a)二次压缩载体图像检测结果



(b)混合二次 JPEG 压缩载密图像检测结果



(c)混合一次 JPEG 压缩图像检测结果

图 3 检测结果

为了进一步对 2 种算法的虚警率进行比较，对未在训练过程中出现的使用其他隐写算法生成的一次 JPEG 压缩载密图像进行了检测。将采用质量因子 Q_1=80 进行一次 JPEG 压缩后的 1 200 张载体图像，使用 JSteg 和 MB 算法分别以嵌入率 25%, 50%, 100%生成不同嵌入率下的一次压缩载密图像，

并运用 2 种算法分别进行检测，结果如图 4 所示。

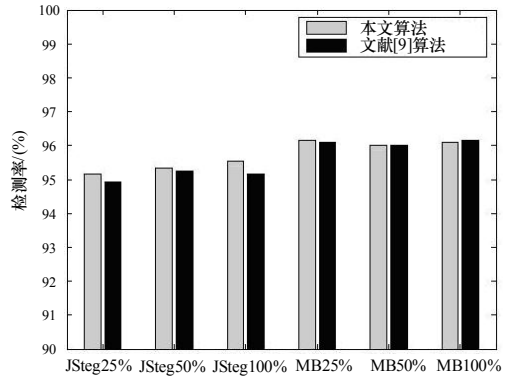


图 4　其他隐写算法虚警率比较

从图 3(c)和图 4 可以明显看出，2 种算法的虚警率都能控制在 5%以内。从图 3(a)和图 3(b)中可以看出，在 Q_1=75 之前，文献[9]的算法和本文的算法相当，检测效果都较好。在 Q_1=80 时，二次 JPEG 压缩的图像可视为一次压缩图像，故 2 种算法的检测结果曲线均在此出现极小值点，但通过比较可以看出本文的算法在 Q_1=Q_2=80 时检测率更高一点。在 Q_1=80 之后，随着 Q_1 越来越大，其对应的量化矩阵在 9 个低频位置{(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(3,1),(3,2),(4,1)}处的量化步长逐步趋近于 1，特别是 Q_1=95 时，9 个位置的量化步长几乎均为 1，很难判断是一次 JPEG 压缩图像还是二次 JPEG 压缩图像，直接导致检测率逐步降低。通过分析还发现，对二次压缩载密图像进行判断时，随着嵌入率的增大，检测率降低。这是因为嵌入的秘密信息越多，对 DCT 系数的统计特性改变越大，使得检测变得越困难。总体来说，在虚警率相当的情况下，本文的算法在 Q_1=80 之后的检测效果要好于文献[9]的算法。

5　结束语

本文算法考虑直流与交流系数的差分在二次 JPEG 压缩过程中的差异变化，在此基础上提出一种新的检测 JPEG 图像二次压缩检测算法。实验结果表明，与文献[9]提出的算法相比，本文算法检测性能更好，能在隐写分析前准确、有效地判断待检测图像是否经过 JPEG 二次压缩。

参考文献

[1] Upham D. JPEG-JSteg-V4[EB/OL]. (2007-05-03). http://www.funet.fi/pub/crypt/stegano- graphy/jpeg-jsteg-v4.diff.gz.

[2] Provos N. OutGuess-practical Steganography[C]//Proc. of UM ACM Computer Security Seminar Series. [S. l.]: ACM Press, 1999.

[3] Westfeld A. F5-A Steganographic Algorithm[C]//Proc. of the 4th International Workshop on Information Hiding. Berlin, Germany: Springer-Verlag, 2001: 289-302.

[4] Sallee P. Model-based Steganography[C]//Proc. of IWDW'04. Seoul, Korea: Springer Verlag, 2004.

[5] 张　涛. 图像隐写分析技术研究[D]. 郑州: 解放军信息工程大学, 2003.

[6] Fridrich J, Goljan M, Hogea D. Steganalysis of JPEG Images: Breaking the F5 Algorithm[C]//Proc. of the 5th Information Hiding Workshop. Noordwijkerhout, Netherlands: [s. n.], 2002.

[7] Fridrich J, Goljan M, Hogea D. Attacking the OutGuess[C]//Proc. of the 11th ACM Workshop on Multimedia and Security. Juan-les-Pins, France: [s. n.], 2002.

[8] Fridrich J. Feature-based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes[C]//Proc. of the 6th Information Hiding Workshop. Saint Malo, France: [s. n.], 2005.

[9] Pevny T, Fridrich J. Detection of Double-compression in JPEG Images for Application in Steganography[J]. IEEE Trans. on Information Forensics and Security, 2008, 3(2): 247-258.

编辑　金胡考

(上接第 139 页)

(6)盲性：只有用户 U 知道 x_u,u_1,u_2，而 $x_u,u_1,u_2 \in Z_q^*$，且 H_1 是安全的哈希函数，因此，除了用户 U，任何人都不能从等式 $y_u = x_u P$，$t_i' = H(m_i \| m_w)$，$t_i = u_1^{-1} t_i' - u_2 y_u$ 得到消息 m_i 的具体信息。

5　结束语

通过匿代理和盲聚合签名的结合，本文方案有效保护了代理签名人的隐私权，并且在事后某签名引发争议时，还可以追踪代理签名人的身份。如何将聚合签名和多代理签名结合，设计更长的签名消息方案尚待研究。

参考文献

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages[J]. IEICE Transactions on Fundamentals, 1996, 79(9): 1338-1354.

[2] 周宣武, 杨晓元, 潘晓中. 基于超椭圆曲线密码的代理授权签名方案[J]. 计算机工程, 2007, 33(24): 170-171.

[3] Liu Yu-Chuan, Wen Hsiang-An, Lin Chun-Li, et al. Proxy-protected Signature Secure Against the Undelegated Proxy Signature Attack[J]. Computers & Electrical Engineering, 2007, 33(3): 177-185.

[4] Zhou Fucai, Zhang Jun, Xu Jian. Research on Anonymous Signatures and Group Signatures[J]. Computer Communications, 2008, 31(17): 4199-4205.

[5] Yu Yong, Xu Chunxiang, Huang Xinyi, et al. An Efficient Anonymous Proxy Signature Scheme with Provable Security[J]. Computer Standards & Interfaces, 2009, 31(2): 88-100.

[6] Chaum D. Blind Signatures for Untraceable Payment[C]// Proceedings of CRYPTO'83. London, UK: [s. n.], 1983: 199-203.

[7] Boneh D, Gentry C, Lynn B, et al. Aggregate and Verfiably Encrypted Signatures from Bilinear Maps[M]. Berlin, Germany: Springer-Verlag, 2003.

[8] Galbraith S D, Harrison K, Soldera D. Implementing the Tate Pairing[M]. [S. l.]: Springer-Verlag, 2002.

编辑　张正兴