

基于差分统计特性的图像置乱度盲评价线性模型

王聪丽^{1,2*}, 陈志斌², 薛明晰², 张超²

(1. 军械工程学院 计算机工程系, 石家庄 050003; 2. 军械工程学院 军械技术研究所, 石家庄 050003)

(* 通信作者电子邮箱 cong7592@tom.com)

摘要:当前大部分图像置乱度评价算法均依赖于原始图像,且缺乏科学的数学模型作为基础。在分析置乱图像差分统计分布特性的基础上,建立了理想置乱图像差分统计分布线性模型,并以此为基础,提出了三种置乱度盲评价算法:斜率绝对差法、差分绝对差法和重叠面积法。实验结果表明:三种算法对于图像差分统计分布有较强的敏感性,且不依赖于原始图像,能客观地评价图像置乱度,与人类视觉系统有着良好的一致性。

关键词:图像置乱;置乱度;盲评价;图像差分;线性模型

中图分类号: TP309.7 **文献标志码:** A

Linear model for blind evaluation of image scrambling degree based on difference statistic distribution

WANG Cong-li^{1,2*}, CHEN Zhi-bin², XUE Ming-xi², ZHANG Chao²

(1. Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang Hebei 050003, China;

2. Ordnance Institute of Technology, Ordnance Engineering College, Shijiazhuang Hebei 050003, China)

Abstract: Most of the current approaches to evaluate the degree of image scrambling depend on original images. And there are no scientific mathematical models as their theoretic basis. A linear model for difference statistic distribution of ideal scrambled image was put forward in this paper by analyzing the difference statistic distribution of scrambled image. Furthermore, three methods were presented based on this model to evaluate image scrambling degree. The first one was the absolute difference of slope, the second was the absolute difference of difference, and the third was method of overlapping area. The experimental results indicate that these methods are very sensitive to the statistical distribution of image difference, and they are independent of original image with good agreement with human vision system, so they can achieve blind evaluation for image scrambling degree objectively.

Key words: image scrambling; scrambling degree; blind evaluation; image difference; linear model

0 引言

图像置乱作为图像加密技术的主要手段,近年来取得了快速发展。如何科学评价置乱算法的效果是当前面临的主要问题。目前,常用的评价方法有主观评价和客观评价。主观评价是由人的视觉感知对置乱图像进行评价,具有简单直观的优点,但是很多主观因素会对评价结果的真实性造成影响。因此,寻找更加科学的客观评价算法具有更重要的实际意义和理论价值。科学的置乱度评价算法应该能达到以下目的:1)能同时度量针对像素位置和像素值变换的加密算法性能;2)应该能够反映置乱图像和所用的置乱算法之间的某种关系,比方说置乱度与置乱次数的关系;3)计算过程应该用到尽可能少的原始图像数据。目前,关于置乱度评价的研究相对比较落后,不能很好地达到上述要求,给实际工作带来了很大的限制。比如,对于目的3),因为原始图像本身就具有特殊性,不具一般性,这就造成置乱度的计算与比较缺乏相同的标准,客观性欠佳。因此,亟须解决的问题是针对理想置乱图像建立科学的统计模型,使所有置乱算法性能评价具有相同的标准,并进一步研究盲评价指标,使得在进行置乱度评价时

无需原始图像的参与,实现准确客观的盲评价。近年来,关于置乱度评价常用的指标有信噪比^[1-2]、距离^[3-4]、熵^[5-6]、统计直方图、质心^[7-8]等,这些指标较单一,大部分属于图像的一阶统计量,均依赖于原始图像,且没有建立比较科学的数学模型。文献[1,9]利用图像的二阶统计量——差分来进行置乱度评价,但是也没有建立科学的模型。本文立足于盲评价指标的设计,从图像差分直方图的统计特性出发,根据实验,建立了理想置乱图像差分直方图的线性模型,并依据该模型提出了三种置乱度盲评价算法。

1 自然图像差分直方图

记自然图像 I 在位置 (i, j) 的灰度值为 $I(i, j)$,考察垂直方向上相邻像素差分的统计分布,即差分图像 $D(i, j) = I(i, j) - I(i, j + 1)$ 的统计分布。一般认为自然图像的差分图像服从广义高斯分布,其概率密度为

$$p_{v,\beta}(x) = \frac{v}{2\beta\Gamma(\frac{1}{v})} \exp\left\{-\left(\frac{|x|}{\beta}\right)^v\right\} \quad (1)$$

其中 v 为形状因子,对于自然图像,一般在0.25和1.5之间。图1(a)、(b)给出了256×256标准灰度图像Lena.bmp和它

收稿日期:2012-06-19;修回日期:2012-07-25。

作者简介:王聪丽(1979-),女,河北定州人,讲师,博士研究生,主要研究方向:信息安全、图像处理; 陈志斌(1965-),男,湖南南县人,研究员,博士生导师,博士,主要研究方向:光电探测、红外目标跟踪与识别、图像加密; 薛明晰(1985-),男,辽宁沈阳人,助理工程师,博士研究生,主要研究方向:光电探测、图像处理; 张超(1988-),男,河北冀州人,助理工程师,硕士研究生,主要研究方向:图像处理、红外目标跟踪与识别。

的差分直方图。

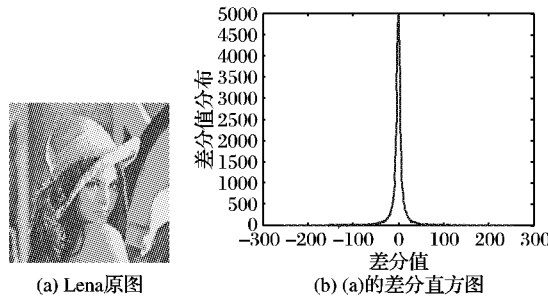


图1 Lena 图像及其差分直方图分布

2 理想置乱图像差分直方图线性模型

由于三维 Arnold 变换^[10]同时实现了对图像像素位置和像素值的置乱,具有代表性。采用灰度级为 256,尺寸为 256×256 的 Lena. bmp 作为实验图像,置乱参数与文献[3]相同。由于置乱 5 次的置乱图像(图 2(a))具有较好的主观视觉效果,直方图分布较均匀(图 2(b)),本文对其进行分析。考察其差分直方图包络图(图 2(c)),其分布已经打破了原来的统计分布特性,差分值的分布有着较强的类线性特性。

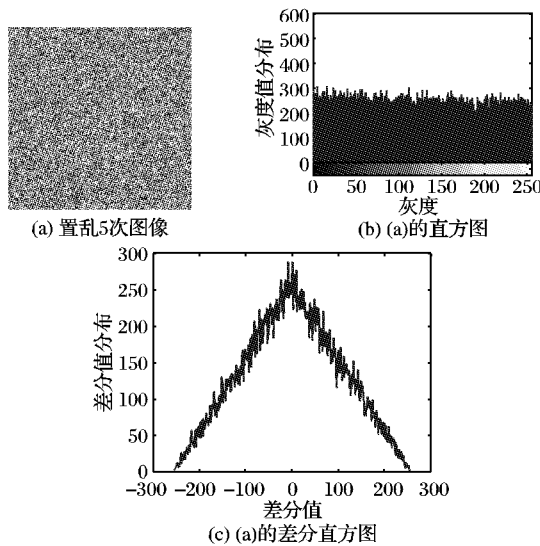


图2 三维 Arnold 变换置乱 5 次图像及其直方图和差分直方图

为了找出该规律的最佳模拟模型,定义 $N(j)$ 为差分为 j 时的差分值个数, $j = -255 \sim 255$, 且 j 为整数。根据线性插值思想,任意两点确定的直线的斜率为:

$$k_{i,j} = (N(j) - N(i)) / (j - i) \quad (2)$$

经过实验验证,对于大部分自然图像来说,满足条件 $N(-255) = N(255) \approx 0$, 因此,选取 $(-255, N(-255))$ 和 $(255, N(255))$ 作为不动点,分别计算 $k_{-255,j}$ ($j = -254 \sim 0$), 和 $k_{j,255}$ ($j = 1 \sim 254$) 并考察其分布。

通过斜率分布图(图 3),我们发现 $k_{-255,j}$ 以 $k = 1$ 为中心上下波动,且逐渐收敛到 1;而 $k_{j,255}$ 以 $k = -1$ 为中心上下波动,逐渐收敛到 -1。由此可得出,对于 $j \leq 0$, 选取 $k = 1$ 作为线性模型的斜率,即理想置乱时的斜率,起点为 $(-255, 0)$, 终点为 $(0, 255)$ 。对于 $j \geq 0$, 选 $k = -1$, 起点为 $(0, 255)$, 终点为 $(255, 0)$ 。由此得到理想置乱情况下图像差分直方图分布模型为:

$$f(x) = \begin{cases} 255 + x, & -255 \leq x < 0 \\ 255 - x, & 0 \leq x < 255 \end{cases} \quad (3)$$

由式(3)可见该模型是一个线性分段函数,自变量为差

分值,函数值为图像差分值个数。该模型表明:理想置乱情况下,置乱图像的差分直方图统计分布曲线应为差分值的线性函数,如图 4 所示。

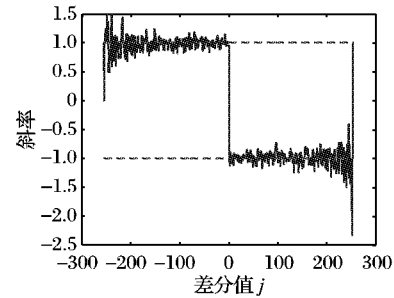


图3 斜率分布图

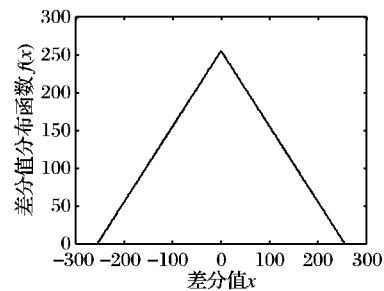


图4 置乱图像差分分布线性模型

对于置乱图像水平和对角方向的差分直方图也用同样的模型来逼近,限于篇幅,不再给出具体分析。

3 评估指标

为了度量置乱图像差分直方图与线性模型的相似度,根据上述模型,提出三种形状相似度因子:斜率绝对差因子、差分绝对差因子和重叠面积因子,并进一步给出了三种图像置乱度盲评价指标。

3.1 斜率绝对差因子

本线性模型以理想置乱时图像差分分布曲线的斜率为基础来建立。为了考察置乱图像与线性模型之间的差别,以斜率绝对差作为度量因子。

定义斜率绝对差因子如下:

$$E_1 = \{E_{1j}\}; j = -254, \dots, 254 \quad (4)$$

$$E_{1j} = \begin{cases} |k_{-255,j} - 1|, & -254 \leq j \leq 0 \\ |k_{j,255} - (-1)|, & 1 \leq j \leq 254 \end{cases} \quad (5)$$

从式(4)、(5)可看出,斜率绝对差因子 E_1 越大,置乱图像差分直方图与线性模型的差别越大,即相似度越低;反之,两者相似度越高。

图像置乱度定义为:

$$\alpha = 1 - \text{mean}(E_1) \quad (6)$$

其中 $\text{mean}()$ 表示取均值。

值得注意的是,当图像的差分直方图与线性模型差别很大时, α 可能取负值。

3.2 差分绝对差因子

置乱图像差分直方图分布与线性模型之间的差别可用两者绝对差来衡量。绝对差越小,说明两者差别越小,相似度越高,图像置乱效果越好。达到理想置乱时,两者分布完全相同,误差为 0。

定义

$$E_{2j} = |N(j) - f(j)| \quad (7)$$

为置乱图像与理想线性模型差分为 j 时的绝对差,则定义

$$E_2 = \sum_j E_{2j} \quad (8)$$

为差分绝对差因子。由此定义

$$\beta = 1 - \frac{E_2}{\sum_j N(j)} \quad (9)$$

为图像置乱度。这里 $\sum_j N(j) = \sum_j f(j)$ 。

3.3 重叠面积因子

置乱图像直方图分布与线性模型相似度还可以用两者分布曲线的重叠面积大小来度量。

下面说明如何计算置乱图像的直方图分布曲线与线性模型曲线的重叠面积。以 $j \leq 0$ 为例, 针对 $N(j)$ 与 $f(j)$ 的大小关系, 有 4 种情况。

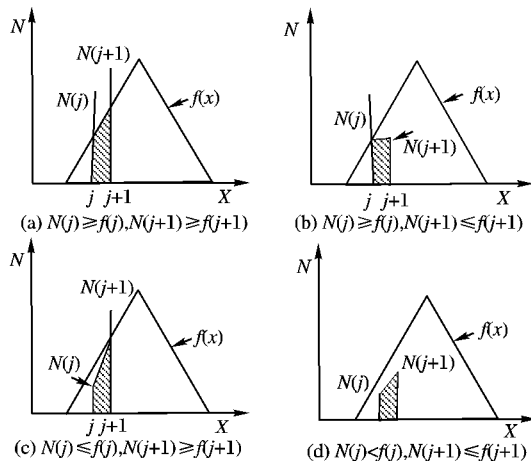


图5 重叠面积计算示意图

为了近似计算重叠面积(即阴影部分的面积), 根据 $f(j)$ 和 $N(j)$ 的大小关系决定的不同情况, 利用梯形面积公式, 可求得每一个阴影部分面积 $S(j)$, 总的重叠面积为 $S = \sum_j S(j)$, 即为重叠面积因子。利用该方法定义的图像置乱

度评价指标为:

$$\gamma = S/S_f \quad (10)$$

其中 S_f 为三角形的面积。

式(10)的物理意义是置乱图像差分直方图与线性模型相交的阴影部分面积占三角形面积的比例。

4 实验结果及分析

为了验证该模型及三种置乱度评价算法的正确性, 本文对 53 幅自然图像分别利用三维 Arnold 变换进行三次置乱变换, 计算置乱图像由上述三种评价算法所求的置乱度分布。如图 6 所示。

通过图 6 可以得出如下结论: 本文提出的模型对于自然图像适用, 能够客观地评价图像的置乱度, 而且三种方法的评价结果具有较高的一致性。

为了进一步验证本文方法对图像差分统计分布的敏感性以及与人类视觉系统(Human Vision System, HVS)的一致性, 对 Lena 图像利用 3 维 Arnold 变换置乱 100 次。考察置乱度的分布曲线, 并与文献[11-12]中的方法进行对比。

从图 7 可以看出, 在给定的参数下, 三维 Arnold 变换的置乱度并不是随着置乱次数的增加而增加, 甚至会出现剧烈下降。比如当置乱次数 $t = 24, 48, 72, 96$ 时, 置乱度出现剧烈下降, 而并不是文献[3]中提到的置乱 10 次后置乱结果没有明显变化。观察上述置乱图像(置乱次数 $t = 24, 48, 72, 96$) 及其差分直方图(见图 8), 我们发现置乱图像具有明显的规律性, 置乱效果较差, 尤其是置乱次数为 96 时, 已经能够在一定程度上分辨出原始图像的内容, 而且其差分直方图与线性模型差别较大。这说明本文模型和置乱度评价指标对图像差分统计分布特征具有较高的敏感度。与其他两种方法相比, 在敏感性及与人类视觉系统的一致性方面, 本文算法最好, 灰色块盲检测算法次之, 图像表面积算法最差。

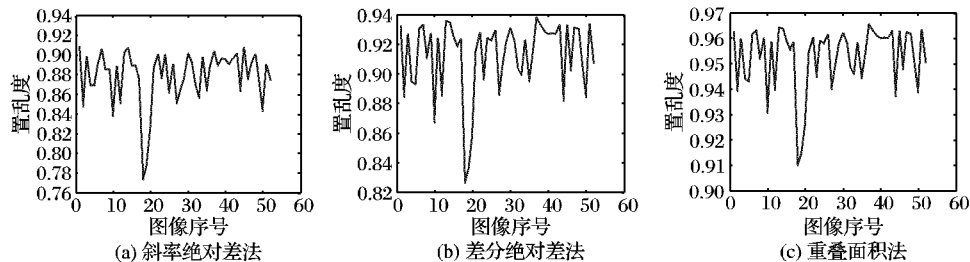


图6 53幅自然图像置乱度分布曲线

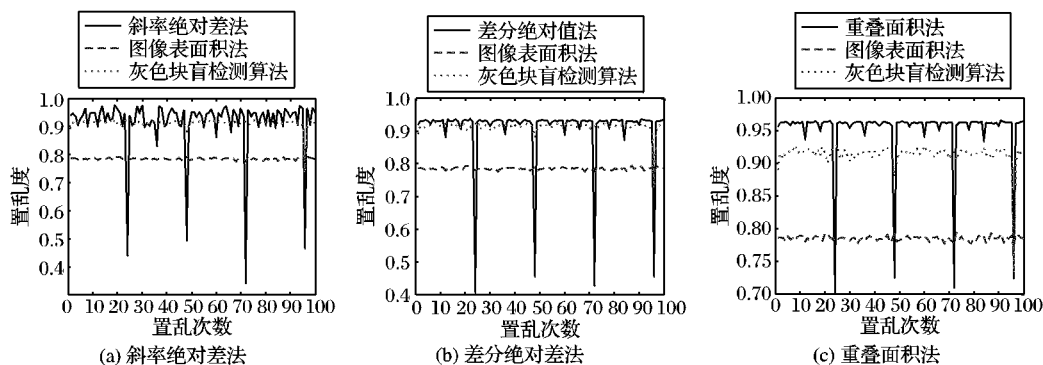


图7 不同评价算法置乱度分布曲线

本文提出的三种算法相比, 根据其相应的定义可知, 斜率绝对差法反映的是置乱图像和线性模型间的斜率差, 在某些情况下会取到负值(一般置乱因子在 $[0, 1]$ 内取值), 科学性欠佳。差分绝对差法和重叠面积法能够科学度量两者之间的差别, 均在 $[0, 1]$ 内取值, 能取得较客观的度量效果。

通过上述分析, 本文提出的三种置乱度评价算法都具有以下特点: 1) 达到理想置乱时, 三者都趋近于 1; 2) 计算量小; 3) 能同时度量像素值和像素位置的置乱; 3) 由于置乱次数不同, 对图像差分的统计分布具有较高的敏感度; 4) 均不依赖于原始图像, 能实现盲评价。

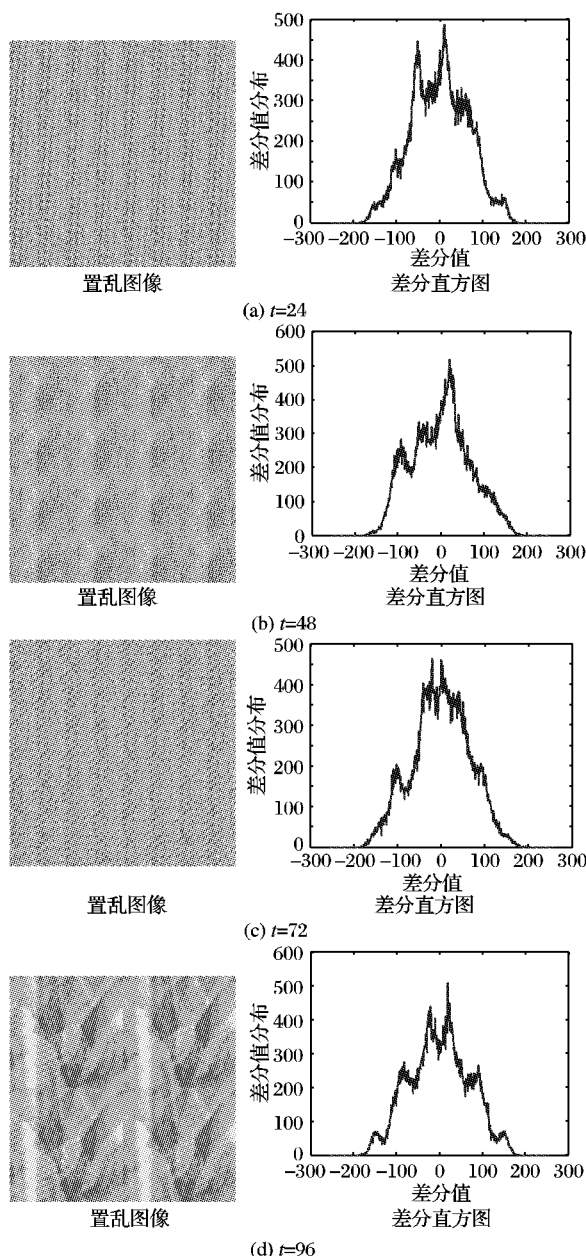


图8 置乱次数 $t=24, 48, 72, 96$ 时的置乱图像及其差分直方图

5 结语

图像置乱度客观评价研究具有非常重要的意义。首先,

它能够客观评价置乱度,弥补主观评价存在的不足;其次,能够为开发高安全性的置乱算法起到指导作用。尤其是盲评价算法能够使得置乱度评价独立于原始图像,因而具有更加重要的实用价值。本文在分析置乱图像差分直方图分布特性的基础上,建立了理想置乱下图像差分直方图线性模型。该模型指出理想置乱情况下,置乱图像的差分直方图分布曲线应为差分值的线性函数。进一步根据该模型提出三种置乱度盲评价算法:斜率绝对差法、差分绝对差法和重叠面积法。实验结果表明,本文模型和评价算法对自然图像适用,对于图像差分统计分布特性有较强的敏感性,和人类视觉系统有着良好的一致性,能够实现置乱度盲评价,为图像置乱度的客观评价工作提供了统一的标准,对于图像置乱度评价工作具有重要的理论意义和实用价值。

参考文献:

- [1] 田小平,吴成茂,谭铁牛. 基于差分信噪比的图像置乱效果评价研究[J]. 计算机工程与设计, 2009, 30(10): 2390-2393.
- [2] 李志伟,陈燕梅,张胜元. 基于 SNR 的数字图像置乱程度评价方法[J]. 厦门大学学报: 自然科学版, 2006, 45(4): 484-487.
- [3] 吴成茂,田小平,谭铁牛. 基于图像距离测度的置乱效果评价方法[J]. 计算机工程与设计, 2009, 30(21): 4891-4894.
- [4] 乔鞣鞣,吴成茂,田小平. 一种图像距离定义及其在置乱效果评价中的应用[J]. 计算机应用, 2010, 30(5): 1338-1343.
- [5] 张华熊,吕辉,翁向军. 基于信息熵的图像置乱程度评价方法[J]. 电路与系统学报, 2007, 12(6): 95-98.
- [6] 田小平,吴成茂,谭铁牛. 运用模糊熵理论进行图像置乱程度评价[J]. 计算机工程与应用, 2009, 45(27): 82-87.
- [7] 周詮,冯新岗. 基于质心的数字图像置乱度衡量准则[J]. 电子与信息学报, 2008, 30(11): 2684-2687.
- [8] ZHAO LIANG, AVISHEK A, SAKURAI K. A new scrambling evaluation scheme based on spatial distribution entropy and centroid difference of bit-plane[C]// Proceedings of the 9th International Conference on Digital Watermarking. Berlin: Springer-Verlag, 2011: 29-44.
- [9] 田小平,吴成茂. 利用差分图像奇异值分解的置乱程度评价研究[J]. 计算机工程与应用, 2010, 46(23): 162-165.
- [10] 吴成茂,田小平. 三维不等长 Arnold 变换及其在图像置乱中的应用[J]. 计算机辅助设计与图形学学报, 2010, 22(10): 1831-1840.
- [11] 王新新,布挺. 基于图像表面面积的置乱程度评价算法[J]. 安徽大学学报: 自然科学版, 2011, 35(4): 48-52.
- [12] 田红鹏. 图像置乱效果盲评价的灰色块分析方法[J]. 计算机工程与应用, 2009, 45(34): 171-173.

(上接第 3469 页)

参考文献:

- [1] CHAUM D, HEYST F. Group signature[C]// Proceedings of EUROCRYPT '91. Berlin: Springer-Verlag, 1991: 257-265.
- [2] 赵泽茂. 数字签名理论[M]. 北京: 科学出版社, 2007: 177-211.
- [3] CAMENISH J, STADLER M. Efficient group signature schemes for large groups[C]// Proceedings of CRYPTO'97. Berlin: Springer-Verlag, 1997: 410-424.
- [4] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret[C]// Proceedings of ASIACRYPT '01. Berlin: Springer-Verlag, 2001: 552-565.
- [5] LV J, WANG X. Verifiable ring signature[C]// Proceedings of the 9th International Conference on Distributed Multimedia Systems. Miami, USA: [s. n.], 2003: 663-665.
- [6] 甘志, 陈克非. 一个新的可验证环签名方案[J]. 中山大学学报: 自然科学版, 2004, 43(22): 132-134.
- [7] SHAMIR A. An identity based cryptosystems and signature scheme[C]// Proceedings of CRYPTO '84. Berlin: Springer-Verlag, 1984: 47-53.
- [8] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// Proceedings of AsiaCRYPTO '03. Berlin: Springer-Verlag, 2003: 452-473.
- [9] 罗大文, 何明星, 李斌. 无证书的可验证环签名方案[J]. 计算机工程, 2009, 35(15): 135-137.
- [10] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, 79(9): 1338-1353.
- [11] 罗大文, 何明星, 李斌. 可验证的代理环签名方案[J]. 西南民族大学学报: 自然科学版, 2009, 35(3): 608-611.
- [12] HERRANZ J, SAEZ G. Forking lemmas for ring signature scheme[C]// Proceedings of IndoCrypt'03. Berlin: Springer-Verlag, 2003: 266-279.