空域中实现基于 DC 系数的图像水印算法*

苏庆堂[1,2], 牛玉刚[1†], 刘贤喜[3]

(1. 华东理工大学 信息科学与工程学院, 上海 200237; 2. 鲁东大学 信息科学与工程学院, 山东 烟台 264025; 3. 山东农业大学 机电工程学院, 山东 泰安 271018)

摘 要: 针对多数图像水印算法是在单一的空域或频域中执行的现状,提出一种结合两者优点的彩色图像盲水印算法。根据 DCT 域中 DC 系数的形成原理,在空域中直接求得亮度分量 Y 中 8×8 子块的 DC 系数并建立其量化表;在空域中通过直接修改像素值实现在 DCT 域中修改 DC 系数来嵌入水印的目的。水印的提取不需要原始水印和原始宿主图像。实验结果表明,该算法既有频域算法鲁棒性高的优点,又有空域算法执行效率高的优点。

关键词: 图像水印; 直流系数; 空域; 离散余弦变换; 彩色图像

中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)04-1441-04

doi:10.3969/j.issn.1001-3695.2012.04.067

Image watermarking algorithm based on DC components implementing in spatial domain

SU Qing-tang[1,2], NIU Yu-gang[1†], LIU Xian-xi[3]

(1. *College of Information Science & Engineering, East China University of Science & Technology, Shanghai* 200237, *China*; 2. *College of Information Science & Engineering, Ludong University, Yantai Shandong* 264025, *China*; 3. *College of Mechanical & Electrical Engineering, Shandong Agricultural University, Tai'an Shandong* 271018, *China*)

Abstract: It was noted that most of the existing watermarking algorithms were performed only in the single spatial domain or frequency domain, this paper proposed a novel blind watermarking algorithm which combining with both advantages for color host images. By utilizing the generating principle and the distribution feature of direct current (DC) coefficient in DCT transformation, firstly, it calculated the DC coefficient of each 8×8 block of the Y luminance directly in spatial domain to create the quantization table. Then, it modified all pixel values of each block to embed watermark in the spatial domain instead of in the DCT domain. In addition, the watermark might be extract from the watermarked image without the original watermark and the original host image. Experimental results show that the proposed method not only has the higher robustness that is the advantage of frequency domain, but also has lower-computation complexity that is the advantage of spatial domain.

Key words: image watermarking; DC coefficient; spatial domain; discrete cosine transform(DCT); color image

0 引言

随着以互联网为代表的信息技术的普及应用,信息安全保护问题日益突出。作为信息隐藏技术的主要分支之一,数字水印技术在实现版权保护和作品真实性鉴别等方面受到研究者的普遍重视[1~3]。

按图像水印的隐藏位置,可将其分为频域水印[4~9]和空域水印[10]。频域水印技术一般是将图像进行频域变换,通过修改其变换系数来嵌入水印,其主要优点是具有较强的鲁棒性;而空域算法通常是将水印嵌入到像素的不重要比特位上,其具有计算简单、复杂度低等优点。由于频域和时域各有不同的优点,因而各自在数字水印中都得到了广泛的应用。但是研究发现,这些应用是在单一的频域或空域中实现的,没有将两者的优点有机结合起来。虽然 Shih 等人[11]提出组合空域和频域的算法,但是并没有真正结合空域和频域的优点来实现水印嵌入,它是在不同条件下来分别选择空域或者频域算法。从原理上讲,频域水印算法是将嵌入的信号能量分布到空域中的所有像素,这意味着可以在空域里直接更新像素的值来完成频域算法的功能。

基于上述讨论,本文提出一种结合两者优点的彩色图像盲水印算法。首先,将原始彩色宿主图像由 RGB 色彩空间转换到 YCrCb,并将其 Y 分量分成大小为 8×8 的像素块;然后,根据 DCT 域中 DC 系数的形成原理,在空域里直接计算每一分块的 DC 系数,并根据水印信息和量化步长来确定每一个 DC 系数的修改量;最后,根据 DC 系数修改量的分布特点,直接在空域中完成水印的嵌入。

本文算法在空域中完成了频域中嵌入水印的过程,避免了频域系数转换形成的误差。实验结果表明,该算法不但具有频域算法鲁棒性强的优点,而且具有空域算法执行效率高的优点。

收稿日期: 2011-10-18; **修回日期**: 2011-12-25 **基金项目**: 国家自然科学基金资助项目(61074041,61170161);国家"十二·五"科技支撑计划重大项目(2011BAD20B01);山东省科技发展计划资助项目(2011YD01079)

作者简介: 苏庆堂(1971-),男,山东烟台人,硕士,主要研究方向为数字水印、信息安全(sdytsqt@163.com);牛玉刚(1964-),男(通信作者),上海人,教授,博导,博士,主要研究方向为随机控制系统、滑模控制、网络控制系统等;刘贤喜(1963-),男,山东日照人,教授,硕导,博士,主要研究方向为计算机虚拟仿真.

1 空域中 DC 系数的修改方法

1.1 空域中获得 DC 系数

给定一幅大小为 $M \times N$ 的图像 $f(x, y)$ ($x = 0,1,2,\cdots, M-1$; $y = 0,1,2,\cdots,N-1$),其 DCT 定义为

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \quad (1)$$

其中:

$$\alpha_u = \begin{cases} \sqrt{1/M} & u = 0 \\ \sqrt{2/M} & 1 \leqslant u \leqslant M-1 \end{cases}, \alpha_v = \begin{cases} \sqrt{1/N} & v = 0 \\ \sqrt{2/N} & 1 \leqslant v \leqslant N-1 \end{cases} \quad (2)$$

同样,其逆 DCT 定义为

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} \alpha_u \alpha_v C(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \quad (3)$$

由式(1)可知,当 $u = 0, v = 0$,即 DCT 域中的 DC 系数 $C(0,0)$可表示为

$$C(0,0) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \quad (4)$$

由式(4)可以看出,DC 系数 $C(0,0)$可以在空域中通过简单的数学运算求得,而无须经过复杂的 DCT 得到。

1.2 空域中修改 DC 系数

在 DCT 的结果中除了一个 DC 系数外,其余的都是 AC 系数,因此,由式(3)所述的 DCT 逆变换可以改写为

$$f(x,y) = \frac{1}{\sqrt{MN}} C(0,0) + f^{AC}(x,y) \quad (5)$$

其中:$f^{AC}(x, y)$是由 AC 分量数据重组的交流成分图像。

假设分块后的原始宿主图像可表示为

$$f(x,y) = \{f_{i,j}(m,n), 0 \leqslant i < M/b, 0 \leqslant j < N/b, 0 \leqslant m,n < b\} \quad (6)$$

其中:M 和 N 表示原始图像的行列尺寸,原始图像被分割成大小为 $b \times b$ 的非重叠块,每一个块的行列坐标为(i, j);m、n 是每个块内的像素点坐标。

假设将嵌入水印 W 嵌入到 DC 系数的第(i, j)个子块,其修改量定义为 $\Delta M_{i,j}$,则 DCT 域中在(i, j)块 DC 系数嵌入水印的过程可以描述为

$$C'_{i,j}(0,0) = C_{i,j}(0,0) + \Delta M_{i,j} \quad (7)$$

$$f_{i,j}'(m,n) = \frac{1}{b} C_{i,j}'(0,0) + f_{i,j}^{AC}(m,n) \quad (8)$$

其中:$C_{i,j}(0,0)$是(i, j)的 DC 系数;$C'_{i,j}(0,0)$是用 $\Delta M_{i,j}$修改后的 DC 系数;$f'_{i,j}(m, n)$是含水印的图像。

不难发现,利用式(6)和(7),式(8)可进一步推导为

$$f_{i,j}'(m,n) = \frac{1}{b} C'_{i,j}(0,0) + f_{i,j}^{AC}(m,n) = \frac{1}{b}(C_{i,j}(0,0) + \Delta M_{i,j}) + f_{i,j}^{AC}(m,n) = \frac{1}{b}\Delta M_{i,j} + f_{i,j}(m,n) \quad (9)$$

式(9)表明,对于宿主图像$f(x, y)$,在 DCT 域中利用 DC 系数来嵌入水印可以直接在空域中实现,也就是说在空域中将 $b \times b$块内的每个像素增加 $\Delta M/b$ 即可嵌入水印。本文用一个 4×4的像素块来举例说明这个过程。原始像素块如图 1(a)所示;当在 DCT 域中的 DC 系数嵌入水印时,则该块执行 DCT 结果,如图 1(b)所示,然后 DC 系数用 $\Delta M = 16$ 来修改;图 1(c)说明了根据式(8)嵌入水印的过程;最后,如图 1(d)所示的含水印的图像块能够通过式(3)的逆 DCT 获得。值得注意的是,图 1(a)与(d)中相对应的像素值之差为 4,即 $\Delta M/b = 16/4 = 4$,根据式(9)能够在空域中由图 1(a)直接获得图 1(d)。

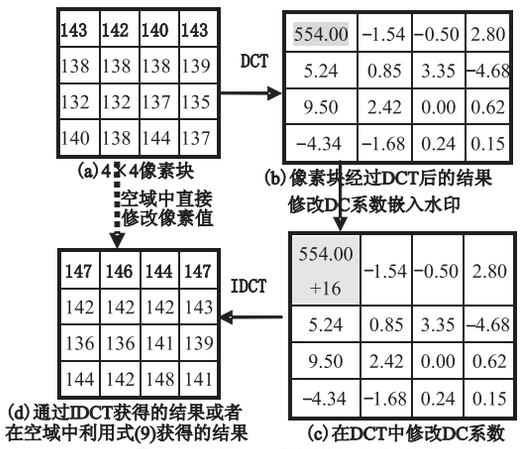

图1 空域中DC系数嵌入水印说明

2 水印算法

2.1 水印生成

本文采用的原始水印 W,如图 2(a)所示,经过基于密钥 K_1 的哈希置乱所得结果如图 2(b)所示,这样进一步提高了水印的鲁棒性和安全性。

(a)原始水印 (b)置乱后的水印

图2 水印预处理

2.2 水印嵌入

水印嵌入的具体步骤描述如下:

a)将宿主图像由 RGB 空间转到 YCrCb 空间。

b)获得 YCrCb 中的 Y 分量,并把它分成大小为 8×8 的非重叠的像素子块。

c)根据式(4),在空域中直接计算每一个子块内的 DC 系数 $C_{i,j}(0,0)$。

d)根据量分表 $QA(k)$ 和 $QB(k)$来量化 DC 系数,量化表的建立是基于密钥 K_2 的量化步长 Δ。

$$QA(k) = \min(C_{i,j}(0,0)) + (2k-4) \times \Delta \quad (10)$$

$$QB(k) = \min(C_{i,j}(0,0)) + (2k-5) \times \Delta \quad (11)$$

其中:$1 \leqslant k \leqslant \text{round}((\max(C_{i,j}(0,0)) + 2\Delta)/(2\Delta)) - \text{round}((\min(C_{i,j}(0,0)) - 2\Delta)/(2\Delta))$,$\min(\cdot)$ 和 $\max(\cdot)$分别定义了量化系数的最小值和最大值,round(·)为取整函数。

e)根据式(12)和(13)计算 DC 系数的修改量 $MC_{i,j}$。

$$C'_{i,j}(0,0) = \begin{cases} QA(k) \text{ if } W(i,j) = 1 \text{ and } \min(C_{i,j}(0,0) - QA(k)) \\ QB(k) \text{ if } W(i,j) = 0 \text{ and } \min(C_{i,j}(0,0) - QB(k)) \end{cases} \quad (12)$$

$$MC_{i,j} = C'_{i,j}(0,0) - C_{i,j}(0,0) \quad (13)$$

其中:$C'_{i,j}(0,0)$是嵌入水印后该块的 DC 系数。

f)利用式(9),将所有像素的值加上 $MC_{i,j}/8$,也就是说,在空域中嵌入了一个水印信息位到这个像素块内。

g)重复执行步骤 c)~f),直到所有的水印嵌入完成,至此得到嵌入水印的 Y 分量,然后将之从 YCrCb 转换到 RGB,最后得到含水印的图像 I'。

2.3 水印提取

在不需要原始宿主图像或原始水印图像的前提下,执行下

列步骤进行水印的提取:

a)转换含水印图像 I' 从 RGB 到 YCrCb 空间。

b)获得 YCrCb 的 Y 分量,并且分割成大小为 8 × 8 的非重叠的像素子块。

c)利用式(4)直接获得 DC 系数 $C_{i,j}(0,0)$。

d)根据式(14),利用基于密钥 K_2 的步长来决定水印 $w'(i,j)$。

$$w'(i,j) = \mathrm{mod}(\mathrm{ceil}(C_{i,j}(0,0)/\Delta),2) \tag{14}$$

e)利用密钥 K_1 对 $w'(i,j)$ 执行哈希逆置乱变换,并获得最终提取水印 W'。

3　实验结果

为了测试本文算法的性能,选取如图 3(a) ~ (d)所示的四幅大小为 512 × 512 的 24 位真彩色图像作为原始宿主图像,选取如图 2(a)所示的大小为 64 × 64 的二值图像作为数字水印,它满足了水印长度最大化的要求。

为了解决水印鲁棒性与不可见性之间的冲突,根据 JPEG 的量化矩阵,选择量化步长 Δ 为 20;为了评估含水印图像的质量,采用峰值信噪比(PSNR)来衡量含水印图像 I' 与原始图像 I 之间的相似度,用归一化相关系数(NC)来衡量所提取的水印 W' 与原始水印 W 之间的相似度。

3.1　水印的不可见性测试

图 3(a) ~ (d)是原始宿主图像,(e) ~ (h)是相应的含水印图像,(i) ~ (l)是从(e) ~ (f)未受攻击时提取的相对应的水印。从图 3(e) ~ (h)可看出,所提算法具有较好的水印不可见性。

图3　原始宿主图像、含水印图像及提取的水印

表 1 为在不同域中利用 DC 系数嵌入水印的比较和未受攻击时提取水印的比较。从表 1 可看到,所提出的基于空域算法要优于基于 DCT 的算法。这是因为基于 DCT 的算法包含 DCT 和逆向 DCT,其中存在数值类型转换、余弦函数计算、矩阵操作、无理数计算等,这些计算误差可以导致较低的计算精度和较大的偏差。同时,本文在 CPU 为 Pentium® D 2.80 GHz,内存为 1.0 GB 的硬件环境下,利用 MATLAB 2010 进行实验得出不同算法的执行时间数据。表 2 为在不同域中执行算法所需的时间比较。从表 2 可以看出,在空域中的执行时间要少于在 DCT 域中的执行时间,这是因为前者的时间复杂度为 $O(N^2)$,而后者的时间复杂度为 $O(N^2\log N)$,所以提出的空域算法要优于基于 DCT 的算法。

表 1　在不同域中利用 DC 系数嵌入水印的比较和未受攻击时提取水印的比较

图像	空域		DCT 域	
	PSNR/dB	NC	PSNR/dB	NC
Baboon	34.605 2	1.000 00	25.929 4	0.980 04
Lena	34.437 8	0.999 45	27.201 0	0.957 90
Peppers	37.825 0	0.995 63	27.654 6	0.935 76
F16	36.358 6	0.998 36	27.418 0	0.954 35

表 2　在不同域中执行算法所需的时间比较　　s

时间	空域	DCT 域
嵌入时间	3.104 4	5.319 6
提取时间	0.390 1	1.809 6
总时间	3.494 5	7.229 2

3.2　鲁棒性测试

为了验证所提算法的鲁棒性,将图 3(e) ~ (h)中四幅含水印的图像进行常见的图像处理(如 JPEG 压缩、加噪攻击、中值滤波攻击和马赛克攻击)和几何攻击(如剪切操作)。

表 3 给出了四幅含水印图像在 JPEG 压缩攻击后所提取的结果。从表 3 中可以看出,当压缩因子为 40% 时,NC 的值足以说明所提水印算法具有较强的鲁棒性。

表 3　含水印图像受 JPEG 压缩攻击后所提取水印的 NC 值

压缩因子	Baboon	Lena	Peppers	F16
30	0.829 1	0.820 1	0.795 8	0.735 9
40	0.985 8	0.963 9	0.950 8	0.952 7
50	0.985 9	0.980 6	0.970 5	0.979 0
60	0.998 6	0.997 0	0.992 6	0.988 5
70	0.999 7	0.999 5	0.994 0	0.998 6
80	0.999 7	0.999 2	0.995 6	0.999 5
90	1.000 0	1.000 0	0.998 4	1.000 0

表 4 是添加不同的椒盐噪声所得的结果。可以看出,所有图像在添加不同因子的噪声后仍然能够提取具有较大 NC 值的水印,这说明了所提算法具有较强的鲁棒性。

表 4　含水印图像受椒盐噪声攻击后所提取水印的 NC 值

噪声参数	Baboon	Lena	Peppers	F16
0.01	0.972 1	0.978 5	0.957 4	0.970 9
0.02	0.937 1	0.942 8	0.934 1	0.930 3
0.03	0.913 9	0.942 3	0.893 7	0.909 0
0.04	0.895 0	0.893 1	0.875 3	0.870 7
0.05	0.860 6	0.871 2	0.866 6	0.848 6

同时,表 5 给出了含水印图像受到其他不同攻击后所提取的水印结果,如马赛克攻击(2 × 2, 3 × 3)、中值滤波攻击(2 × 2, 3 × 3)、Butterworth 低通滤波攻击(截止频率为 50 Hz,级别 n = 2, 3)。从表 5 可以看出,所提取的大部分水印的 NC 值接近于 1,这意味着所提算法对大部分常用的攻击具有较强的鲁棒性。

表 5　含水印图像受到其他不同攻击后所提取水印的 NC 值

攻击方式	Baboon	Lena	Peppers	F16
Mosaic 2 × 2	0.998 4	0.995 6	0.986 3	0.991 8
Mosaic 3 × 3	0.815 8	0.824 2	0.824 2	0.851 3
Median filtering 2 × 2	0.997 8	0.992 9	0.991 7	0.990 1
Median filtering 3 × 3	0.964 8	0.913 6	0.947 5	0.877 8
BLPF n = 2,50 Hz	0.846 1	0.907 5	0.942 0	0.901 7
BLPF n = 3,50 Hz	0.826 1	0.900 1	0.941 0	0.900 5

进一步验证所提算法抵抗几何攻击的鲁棒性。图 4(a) ~ (h)是含水印的 Lena 图像受到不同位置、不同尺寸的剪切结果,4(i) ~ (p)分别给出了从相应的剪切图中所提取的水印,从所提取水印的视觉效果及其 NC 值可以看出,所提算法具有较强的鲁棒性。

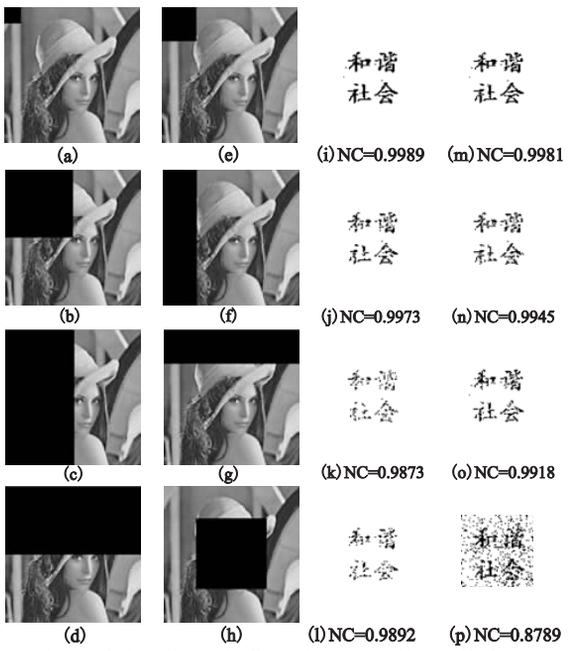

图4 含水印的Lena图像受到不同位置剪切后的结果及所提取的水印结果

总之,由表 3 ~5 和图 4 的实验可以看出,本文算法具有较强的鲁棒性。

4 结束语

本文提出一种新的彩色图像盲水印技术,其突出的优点是:a)用空域技术代替 DCT 域技术将数字水印嵌入在 DC 系数中,与 DCT 域算法相比,所提算法的执行时间减少了一半,并且减少了计算误差,提高了算法的性能;b)利用基于密钥 K_1 的哈希置乱和基于密钥 K_2 的量化步长,水印算法的安全性得到了保障;c)所提算法不但具有较强的鲁棒性,而且算法简单,能够在空域中达到盲提取的目的。

参考文献:

[1] 苏庆堂. 基于整型小波变换的彩色图像盲水印算法[J]. 计算机应用研究, 2009,26(6):2168,2169-2172.

[2] LOU D C, TSO H K, LIU J L. A copyright protection scheme for digital images using visual cryptography technique[J]. Computer Standards & Interfaces,2007,29(1):125-131.

[3] FLEET D J, HEEGER D J. Embedding invisible information in color images[J]. IEEE Trans on Image Processing,1977,1(1):532-535.

[4] QI Xiao-jun, QI Ji. A robust content-based digital image watermarking scheme[J]. Signal Processing,2007,87(6):1264-1280.

[5] USMAN I, KHAN A. BCH coding and intelligent watermark embedding: employing both frequency and strength selection[J]. Applied Soft Computing,2010,10(1):332-343.

[6] LIN S D, SHIE S C, GUO Jian-yi. Improving the robustness of DCT-based image watermarking against JPEG compression[J]. Computer Standards & Interfaces,2010,32(1-2):54-60.

[7] SAMI B, LALA K, THAWAR A, *et al*. Watermarking of digital images in frequency domain[J]. International Journal of Automation and Computing,2010,7(1):17-22.

[8] LIU Lian-shan, LI Ren-hou, GAO Qi. A new watermarking method based on DWT green component of color image[C]//Proc of International Conference on Machine Learning and Cybernetics. 2004: 3949-3954.

[9] LIU Kuo-cheng. Wavelet-based watermarking for color images through visual masking [J]. AEU-International Journal of Electronics and Communications,2010,64(2):112-124.

[10] CHAN C K, CHENG L M. Hiding data in images by simple LSB substitution [J]. Pattern Recognition,2004,37(3):469-474.

[11] SHIH F Y, WU S Y T. Combinational image watermarking in the spatial and frequency domains[J]. Pattern Recognition,2003,36(4):969-975.

(上接第 1433 页)

4 效率分析

新的方案与已有随机预言模型下可证明安全的使用双线性对运算的基于证书签名方案所使用的运算比较分析如表 1 所示。其中,M 表示群 G_1 或 G_2 上的形如 aP 的标量乘法;SM 表示群 G_1 或 G_2 上形如 $aP+bQ$ 的标量乘法;E 表示指数运算;P 表示双线性对运算。

表 1 与已有基于证书签名方案的运算效率比较

方案	签名算法	验证算法	签名长度
文献[2]	$3M$	$3P$	$\|G_1\|\times\|G_1\|\times\|Zq\|$
文献[3]	$1M+2SM$	$3P$	$\|G_1\|\times\|G_1\|$
文献[5]	$1E+2M+2P$	$1M+3P+1E$	$\|G_1\|\times\|Zq\|$
本文	$3M$	$1M+2SM+2P$	$\|G_1\|\times\|G_1\|$

从表 1 可以看出,新的基于证书签名方案无论计算效率还是签名长度均不高于已有可证明安全的基于证书签名方案。

5 结束语

本文提出了一个新的基于证书的数字签名方案。利用随机预言模型,在基于 CDH 问题是难解的假设下,证明了方案的安全性。经过效率比对分析,新的方案设计简单,运算效率高,适用于实际使用,特别是计算能力受限的设备。目前,对基于证书数字签名的研究还不够深入,事实上,如何利用 CDH 问题以及 BDH(判定 Diffie-Hellman)问题(包括它们的变形)的难解性,来设计更多可证安全、有效的基于证书签名方案是一个有意义的课题,也是下一步要研究的工作。

参考文献:

[1] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]//Lecture Notes in Computer Science, vol2656. Berlin: Springer-Verlag, 2003: 272-293.

[2] KANG B G, PARK J H, HAHN S G. A certificate-based signature scheme[C]//Lecture Notes in Computer Science, vol2964. Berlin: Springer-Verlag, 2004: 99-111.

[3] LI Ji-guo, HUANG Xin-yi, MU Yi, *et al*. Certificate-based signature: security model and efficient construction[C]//Lecture Notes in Computer Science, vol4582. Berlin: Springer-Verlag, 2007: 110-125.

[4] LIU J K, BAEK J, SUSILO W, *et al*. Certificate-based signature schemes without pairings or random Oracles[C]//Lecture Notes in Computer Science, vol5222. Berlin: Springer-Verlag, 2008: 285-297.

[5] 王雯娟,黄振杰,郝艳华. 一个高效的基于证书数字签名方案[J]. 计算机工程与应用,2011,47(6): 89-92.