第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 博士论文 •　　文章编号：1000—3428(2011)24—0018—04　　文献标识码：A　　中图分类号：TP393

基于双线性对的无证书签名与群签名方案

李凤银[1,2]，刘培玉[1]，朱振方[1]

(1. 山东师范大学信息科学与工程学院，济南 250014；2. 曲阜师范大学计算机科学学院，山东 日照 276826)

摘　要：传统数字签名方案的证书存储和管理开销较大，基于身份的数字签名方案无法解决其固有的密钥托管问题，而无证书签名方案无需使用公钥证书，且没有密钥托管问题。为此，提出一个基于双线性映射的无证书签名方案，并在随机预言机模型下证明其安全性。在此基础上设计一个无证书群签名方案，其安全性建立在计算 Diffie-Hellman 问题的困难性假设上。性能分析表明，2 种签名方案在保证安全性的前提下，具有较高的执行效率。

关键词：无证书密码体制；群签名；双线性映射；Diffie-Hellman 问题；随机预言机

Certificateless Signature and Group Signature Schemes Based on Bilinear Pairings

LI Feng-yin[1,2], LIU Pei-yu[1], ZHU Zhen-fang[1]

(1. School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China;
2. College of Computer Science, Qufu Normal University, Rizhao 276826, China)

【Abstract】Traditional digital signature schemes need much more storage and management overhead for the use of certificates, while the identity-based digital signature schemes fail to solve the inherent key-escrow problem. Certificateless signature schemes need no certificates and can solve the key-escrow problem. This paper presents a certificateless signature scheme from bilinear pairings, and verifies its security under the random oracle machine. It designs a certificateless group signature scheme from the certificateless signature scheme, and its security is founded under the assumption of the computational Diffie-Hellman problem. Performance analysis shows that both signature schemes are secure and have high performing efficiency.

【Key words】certificateless cryptography; group signature; bilinear mapping; Diffie-Hellman problem; random oracle machine

DOI: 10.3969/j.issn.1000-3428.2011.24.007

1 概述

无证书密码体制的概念由 Al-Riyami S S 和 Paterson K G 于 2003 年提出[1]，既能解决基于身份的公钥系统所固有的密钥托管问题，又能保持其不需使用公钥证书的优点。于是，无证书密码体制以其安全、高效的特性受到密码学界的广泛关注。一些无证书签名和群签名方案[2]应运而生。群签名的概念由 Chaum D 和 Heyst V E 于 1991 年提出[3]，它以独特的性质引起人们的关注并被广泛研究。群签名允许群体中任一成员代表整个群体对消息进行匿名签名。群签名可以公开验证，且在发生纠纷时，群管理员可以打开群签名以揭露签名者的真实身份。但在具体实现中，基于传统密码体制的群签名方案无法避免对所涉及的公钥证书的存储、传输及管理等所带来的额外开销。为克服这个不足，文献[4]提出基于身份的群签名方案。但基于身份的公钥系统所固有的密钥托管问题，对该体制下的群签名方案构成了潜在的安全威胁。文献[2]给出了无证书群签名方案，但其方案不仅使用了零知识证明协议，而且签名和验证的运算代价都很高。本文基于双线性映射设计出一个新的无证书签名方案，并利用随机预言机模型证明了它的安全性。基于该无证书签名方案，本文设计出一个无证书群签名方案。在计算 Diffie- Hellman(CDH)问题的困难性安全假设下，该群签名方案是安全而高效的。

2 预备知识

2.1 双线性映射及数学困难问题

定义 1 双线性映射。假设 G_1 是一个阶为大素数 q 的加法循环群，G_2 是一个阶为 q 的乘法循环群。若映射 $e: G_1\times G_1\to G_2$ 满足以下 3 条性质，则称这个映射为双线性映射。

(1)双线性：对于任何 $U,V\in G_1$，$a,b\in Z_q^*$，$e(aU,bV)=e(U,V)^{ab}$。

(2)非退化性：存在 $U,V\in G_1$，使 $e(U,V)\neq 1_{G_2}$。

(3)可计算性：对于任何的 $U,V\in G_1$，存在一个高效的算法计算 $e(U,V)$ 的值。

定义 2 离散对数问题。给定一个阶为 q 的循环群 G，它的一个生成元 g 以及 $h\in G$，找到一个值 $a\in Z_q^*$ 使得 $h=g^a$。

定义 3 计算 Diffie-Hellman 问题。给定一个阶为 q 的循环群 G，它的一个生成元 P 以及 $aP,bP\in G$ (其中，$a,b\in Z_q^*$ 且其值未知)，计算 $abP\in G$。

2.2 无证书签名方案

一个无证书签名方案由系统参数生成、部分密钥生成、设置秘密值、设置私钥、设置公钥、签名以及验证 7 个算法组成。限于篇幅，具体算法参阅文献[2]。

基金项目：国家自然科学基金资助项目(60873247)；山东省自然科学基金资助重点项目(ZR2009GZ007)；山东省高新技术自主创新工程基金资助项目(2008ZZ28)

作者简介：李凤银(1974－)，女，副教授、博士研究生，主研方向：信息安全，数字签名；刘培玉，教授、博士生导师；朱振方，博士研究生

收稿日期：2011-03-18　**E-mail：**lfyin318@126.com

2.3 安全模型

在无证书系统中有 2 类攻击者，即第 1 类攻击者 A_{I} 与第 2 类攻击者 A_{II}。第 1 类攻击者不知道系统主密钥，但是可以任意替换用户的公钥。第 2 类攻击者知道系统的主密钥，但是不能替换目标用户的公钥。

无证书签名方案的安全性可用挑战者 C 和攻击者 A_{I} 或 A_{II} 间的 2 个游戏[5]定义。

定义 4 一个无证书签名方案在适应性选择消息攻击下是存在不可伪造的，当且仅当任何计算能力多项式受限的攻击者赢得以上 2 个游戏的概率是可以忽略的。

在下文中说一个签名方案是安全的，即指它在适应性选择消息攻击下是存在不可伪造的。

3 基于双线性对的无证书签名方案

3.1 签名方案

签名方案的具体步骤如下:

(1)系统参数生成

输入一个安全参数 k，KGC 选定满足 2.1 节所述性质的 e,G_1,G_2，选定 P 为 G_1 的一个生成元，计算 $g=e(P,P)$，并随机选取 $s\in Z_q^*$作为系统主密钥 mk，记 $P_0=sP$，选择 Hash 函数 $H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_q^*$。

设置系统安全参数 $params=\{e,G_1,G_2,P,P_0,g,H_1,H_2\}$。

(2)部分私钥生成

KGC 利用系统主密钥帮用户生成部分私钥。当输入一个用户的身份 ID，KGC 计算并输出该用户的部分私钥 $D_{ID}=s\cdot Q_{ID}=s\cdot H_1(ID)$。

(3)设置秘密值

用户随机选取 $x\in Z_q^*$中的一个值作为其秘密值。

(4)设置私钥

身份为 ID 的用户设置其私钥为 $S_{ID}=x\cdot D_{ID}$，其中，x 为该用户的秘密值；D_{ID} 为其部分私钥。

(5)设置公钥

秘密值为 x 的用户(身份为 ID)设置其公钥为 $P_{ID}=x\cdot P_0$。

(6)签名

假设签名者的身份为 ID，公钥为 P_{ID}，私钥为 $S_{ID}=x\cdot D_{ID}$，当输入一个消息 M，该签名者按以下方式对消息 M 进行签名：1)随机选取 $r\in Z_q^*$，计算 $R=g^r$；2)计算：$h=H_2(M\,\|\,ID\,\|\,R\,\|\,P_{ID})$，$V=r\cdot P+h\cdot S_{ID}\in G_1$；3)输出签名 $\sigma=(h,V)$。

(7)验证

验证者按如下方式验证身份为 ID，公钥为 P_{ID} 的用户对消息 M 的签名 σ 是否有效。计算 $R'=e(V,P)\cdot e(Q_{ID},P_{ID})^{-h}$，然后检验等式 $h=H_2(M\,\|\,ID\,\|\,R'\,\|\,P_{ID})$ 是否成立，当且仅当等式成立，承认签名为合法签名，输出 1；否则签名非法，输出 0。

3.2 安全性证明

下面利用文献[6]方法对本文方案进行安全性证明。

定理 1 在随机预言机模型下，若群 G_1 中的 CDH 问题是困难的，那么 3.1 节中所构造的无证书签名方案对于第 1 类攻击者是安全的。

证明：假设 C 想解决 G_1 中的 CDH 问题，其输入为(aP, bP)，他需要计算出 abP。假设 A_{I} 是第 1 类攻击者，他能以不可忽略的概率攻破本文签名方案。下面证明 C 能够利用 A_{I} 的能力解决 CDH 问题。

(1)参数设置

参照 3.1 节 C 设置系统参数 $params=\{e,G_1,G_2,P,P_0,g,H_1,H_2\}$，其中，$P_0=a\cdot P$，并将系统参数传给 A_{I}。这里将 Hash 函数 H_1 和 H_2 看成随机预言机。

C 为响应 A_{I} 的 H_1 询问、H_2 询问、部分私钥询问、公钥询问、公钥替换询问、秘密值询问和签名询问，必须维护以下 3 个列表：列表 H_1^{list}，其每一项的格式为 $(ID,\alpha,Q_{ID},D_{ID})$；列表 H_2^{list}，其格式为 (M,ID,R,P,h)；列表 K^{list}，其格式为 (ID,x,P_{ID})。限于篇幅，此处仅给出公钥替换询问和签名询问，其余参阅文献[5]。

(2)公钥替换询问

当 C 接收到 A_{I} 的关于用户 ID_i 的公钥替换询问 (ID_i,P_i') 时，C 检索 K^{list} 找到 (ID_i,x_i,P_i)，设置 x_i=⊥、$P_i=P_i'$。

(3)签名询问

当 A_{I} 请求公钥为 P_i，身份为 ID_i 的用户对消息 M_i 的签名时，C 按照如下步骤回答：1)随机选择 $h_i\in Z_q^*$、$V_i\in G_1$；2)计算 $R_i=e(V_i,P)\cdot e(Q_i,Y_i)^{-h_i}$，其中，$Q_i=H_1(ID_i)$；3)设置 $H_2(M_i,ID_i,R_i,P_i)=h_i$；4)返回$(h_i, V_i)$。

最后，A_{I} 输出一个伪造 $(M^*,\sigma^*=(h,V),ID^*,P^*)$。若 $ID^*\neq ID_J$，C 终止；否则，C 选择另一个 Hash 函数 H_2' 并再次利用 A_{I} 的能力，可以得到另一个伪造 $(M^*,\sigma^{*\prime}=(h',V'),ID^*,P^*)$。从而 C 得到 2 个有效的伪造，并且它们满足 $R=e(V,P)\cdot e(Q,Y)^{-h}$ 与 $R=e(V',P)\cdot e(Q,Y)^{-h'}$。其中，$Q=H_1(ID^*)=bP$，并以 (ID_J,α_J,Q_J,D_J) 的形式存在于 H_1^{list} 中。这样就有等式 $e(V,P)\cdot e(Q,Y)^{-h}=e(V',P)\cdot e(Q,Y)^{-h'}$ 成立，C 可以计算出 CDH 问题的解 $abP=\beta^{-1}(h-h')^{-1}\cdot(V-V')$。证毕。

定理 2 在随机预言机模型下，若群 G_1 中 CDH 问题是困难的，则本文无证书签名方案对于第 2 类攻击者是安全的。

证明：假设 C 是一个 CDH 困难问题的解决者，问题的输入为(aP, bP)，他的目标是计算 abP。假设 A_{II} 是第 2 类攻击者，他能以不可忽略的概率攻破本文签名方案。下面证明 C 能够利用 A_{II} 的能力解决 CDH 问题。

(4)参数设置

参照 3.1 节 C 选择系统主密钥 $s\in Z_q^*$，计算 $P_0=sP$，设置系统参数 $params=\{e,G_1,G_2,P,P_0,g,H_1,H_2\}$，并将 $params$ 与 s 传给 A_{II}。同样将 Hash 函数 H_1 和 H_2 看成随机预言机。

C 为了响应 A_{II} 的公钥询问、H_1 询问、H_2 询问、秘密值询问、公钥替换询问和签名询问，必须维护以下 3 个列表：列表 H_1^{list}，其每一项的格式为 $(ID,\alpha,Q_{ID},D_{ID})$；列表 H_2^{list}，其格式为 (M,ID,R,P,h)；列表 K^{list}，其格式为 (ID,x,P_{ID})。限于篇幅，此处仅给出签名询问，其余参阅文献[5]。

(5)签名询问

当 A_{II} 向 C 请求身份为 ID_i，公钥为 P_i 的用户对消息 M_i 的签名时，C 按照如下步骤回答：1)随机选择 $h_i\in Z_q^*$、$V_i\in G_1$；2)计算 $R_i=e(V_i,P)\cdot e(Q_i,P_i)^{-h_i}$，其中，$Q_i=H_1(ID_i)$；3)设置 $H_2(M_i\,\|\,ID_i\,\|\,R_i\,\|\,P_{ID})=h_i$；4)返回$(h_i, V_i)$。

最后，A_{II} 输出一个伪造 $(M^*,\sigma^*=(h,V),ID^*,P^*)$，若 $ID^*\neq ID_J$，C 终止；否则，C 选择另一个 Hash 函数 H_2' 并再次利用 A_{II} 的能力，它可以得到另一个伪造 $(M^*,\sigma^{*\prime}=(h',V'),ID^*,P^*)$，从而 C 得到 2 个有效的伪造，并且它们满足

$R=e(V,P)\cdot e(Q,P^*)^{-h}$ 与 $R=e(V',P)\cdot e(Q,P^*)^{-h'}$。其中，$Q=H_1(ID^*)=bP$，并以 (ID_J,α_J,Q_J,D_J) 的形式存在于 H_1^{list} 中。于是有等式 $e(V,P)\cdot e(Q,P^*)^{-h}=e(V',P)\cdot e(Q,P^*)^{-h'}$ 成立，从而有 $e(V-V',P)=e(Q,P^*)^{h-h'}$，由设置可知 $e(V-V',P)=e(bP,asP)^{h-h'}$，因此，$C$ 可以计算出 CDH 问题的解 $abP=s^{-1}\cdot(h-h')^{-1}\cdot(V-V')$。证毕。

3.3 效率分析

考虑到双线性映射运算是低效操作，在本文无证书签名方案中，成功地通过采取以下措施提高了签名方案的效率：在参数生成阶段通过一个双线性映射的预处理，减少签名阶段和签名验证阶段双线性映射运算的次数。

在计算和通信效率方面，对本文方案与目前的一些典型无证书签名方案进行比较。用 P 表示一个双线性对运算，S 表示群 G_1 中的一个标量乘运算，E 表示群 G_2 中的一个幂运算，H 表示一个 Hash 到群 G_1 的运算。用 P_1 表示 G_1 中的一个点的长度，用 P_2 表示 G_2 中的一个点的长度，用 Z_1 表示 Z_q^* 中的一个点的长度。比较结果如表 1 所示。数据显示，本文无证书签名方案是安全高效的。

表 1 无证书签密方案与其他签名方案的性能比较

方案	签名	验证(预运算)	签名长度	公钥长度
文献[7]方案	S, $2E$	$1P$, $1S$, $2E(1P,2E)$	$2Z_1$, $1P_1$	$1P_2$
文献[8]方案	$2S$, $1E$	$3P$, $1H(1P,1E)$	$1Z_1$, $1P_1$	$1P_1$
本文无证书签名方案	$2S$, $1E$	$2P$, $1S(1E)$	$1Z_1$, $1P_1$	$1P_1$

4 基于双线性对的无证书群签名方案

利用 3.1 节中的无证书签名方案设计群签名方案如下：

(1)系统参数生成

同 3.1 节的系统参数生成算法。

(2)用户公私钥生成

部分私钥提取，设置秘密值，生成公钥，同 3.1 节的生成私钥算法。

(3)创建

设群管理员(GM)的身份为 ID_G，私钥为 $S_G=x_G\cdot D_G$，公钥为 $P_G=xG\times P_0$，设置群公钥为(ID_G,P_G)。

(4)加入

设用户 Alice 的身份为 ID_A，私钥为 $S_A=x_A\cdot D_A$，公钥为 $P_A=x_A\times P_0$。用户 Alice 想加入群，她与 GM 执行以下协议：

1)Alice 独立地随机选取 $r_A\in Z_q^*$ 作为群签名私钥，并妥善保存，计算 $R_A=g^{r_A}\in G_2$ 作为群签名公钥。计算 $h^A=H_2(R_A\|ID_A\|\|\mathrm{P}_A)$，$\sigma^A=r_A\cdot P+h^A\cdot S_A$，并将 $(ID_A,R_A,\sigma^A,\mathrm{P}_A)$ 发送给 GM。

2)GM 收到 (ID_A,R_A,σ^A,P_A) 后，先计算 $R_A'=e(\sigma^A,P)\cdot e(Q_A,P_A)^{-h^A}$，然后检验等式 $h^A=H_2(R_A'\|ID_A\|\|\mathrm{P}_A)$ 是否成立。当且仅当该等式成立 GM 转向步骤 3)，给 Alice 颁发成员证书；否则，转向步骤 1)，要求 Alice 重新发送数据。

3)GM 为 Alice 生成成员证书，他对 R_A 作签名：计算 $h^{cer_A}=H_1(R_A\|ID_G\|P_G)$、$U^{cer_A}=D_G+S_G\cdot h^{cer_A}$，将成员证书 $cer_A=(U^{cer_A},h^{cer_A})$ 发送给 Alice，同时，把 $(ID_A,R_A,\sigma^A,cer_A)$ 加入成员列表。

4)Alice 收到 cer_A 后，验证等式 $e(U^{cer_A},P)=e(Q_G,P_0)\cdot e(Q_G,P_G)^{h^{cer_A}}$ 是否成立。当且仅当等式成立接收成员证书 cer_A；否则返回步骤 3)，要求 GM 重新发送成员证书，直到上式成立。这样，Alice 成为群成员，并获得成员证书 cer_A。

(5)群签名

成员 Alice 对消息 $M\in\{0,1\}^*$ 签名，用她拥有的成员证书 cer_A 及对应的签名公钥 R^A，签名私钥 r_A 计算 $h=H_2(M\|R^A\|ID_A\|\|P_A)$、$V=r_A\cdot P+h\cdot U^{cer_A}$，输出群签名 $\sigma=(h,V,R^A,h^{cer_A})$。

(6)验证

对于消息 $M\in\{0,1\}^*$，群签名 $\sigma=(h,V,R^A,h^{cer_A})$ 及群公钥 (ID_G,P_G)，验证者首先计算 $h^{cer_A}{}'=H_1(R_A\|ID_G\|P_G)$，然后检验等式 $e(V,P)=R^A\cdot e(Q_G,P_0)^h\cdot e(Q_G,P_G)^{h\cdot h^{cer_A}{}'}$ 是否成立。当且仅当等式成立，接收群签名；否则，拒绝群签名。

(7)打开

对于群签名 $\sigma=(h,V,R^A,h^{cer_A})$，在发生纠纷时，GM 根据保存的成员列表信息 $(ID_A,R_A,\sigma^A,cer_A)$，计算 $R_A'=e(\sigma^A,P)\cdot e(Q_A,P_A)^{-h^A}$，验证 $h^A=H_2(R_A'\|ID_A\|P_A)$ 确定真正的签名者。

(8)成员撤消

GM 维护成员列表，当成员 Alice 要离开群时，向 GM 提出申请。GM 对成员列表中成员 Alice 对应的成员信息打上“时间戳”标记，注明离开时间，撤消该成员。

5 群签名方案的安全性与效率分析

5.1 不可伪造性

群签名方案的安全性基于前面所构造的无证书签名方案的安全性。

引理 若 CDH 问题是困难的，则生成群签名所用无证书签名方案对于第 1 类攻击者 A_{I} 和第 2 类攻击者 A_{II} 是安全的。

群签名的生成基于 3.1 节构造的无证书签名方案，其安全性已经证明，证明过程见 3.2 节。由引理可得定理 3。

定理 3 若 CDH 问题是困难的，则该无证书群签名方案对第 1 类攻击者和第 2 类攻击者是安全的。

5.2 匿名性

给定合法的群签名 $\sigma=(h,V,R^A,h^{cer_A})$，因为 h,V,R^A,h^{cer_A} 中都不含有特定签名者的身份信息，所以除了 GM，其他任何人想确定签名者的真正身份在计算上是不可行的。

5.3 可追踪性

由群签名的不可伪造性可知，只有群成员才能产生合法群签名。每个群成员对应唯一的成员证书，每个群签名都对应唯一的签名者。由于和每个签名者对应的信息早在其签发的群签名生成之前已经存在并被 GM 保存，因此签名者不能阻止一个合法群签名被打开。

5.4 防陷害性

由群签名的不可伪造性可知，任何人(包括群管理员)都不能冒充其他群成员作出合法的群签名。因为其他任何人都无法伪造该群成员在申请成员证书时所生成的签名。

5.5 抗联合攻击性

若一些群成员联合起来想伪造群签名，则由加入协议可知，他们必须通过伪造成员证书达到目的。而基于 CDH 问题，成员证书是不可伪造的。

5.6 无关联性

除了群管理员，任何人想判断 2 个或 2 个以上的群签名是否由同一个群成员产生在计算上是不可行的。

但本文群签名方案并不满足无关联性，不过有很多场合正好用到这种特性，例如在电子投票中，正好需要这种特性保证每个人都没有重复投票；而在有奖举报中需要这种特性

保证举报人没有重复举报。

5.7　效率分析

利用文献[9]方法，在计算和通信效率方面，把本文所设计的群签名方案与一些目前被证明是安全的群签名方案进行比较。用 P 表示一个双线性对运算，S 表示群 G_1 中的标量乘运算，E 表示群 G_2 中的幂运算，H 表示一个 Hash 到群 G_1 的运算。用 P_1 表示 G_1 中的一个点的长度，用 P_2 表示 G_2 中的一个点的长度，用 Z_1 表示 Z_q^* 中的一个点的长度。比较结果如表 2 所示。数据显示，本文方案的签名长度最短，签名、验证和打开算法的效率比其他方案更高。

表 2　3 个群签名方案的性能比较

方案	签名	验证	打开	签名长度	公钥长度	密码系统
文献[2]方案	$7S$	$11P$, $1S$	逐一寻找并验证	$9P_1$	$4P_1$	无证书系统
文献[10]方案	$3S$, $2H$	$4P$, $1S$, $2H$	直接找到 $4P$, $1H$	$4P_1$, $1\|T\|$	P_1, $1\|T\|$	基于身份的系统
本文无证书群签名方案	$2S$	$3P$, $2E$, $1H$	直接找到 $2P$, $1H$, $1E$	$2P_1$, $1P_2$	P_1, $\|ID_G\|$	无证书系统

6　结束语

本文设计一个无证书签名方案，并在随机预言机模型下证明其安全性。基于该无证书签名方案，设计一个群签名方案，该群签名方案满足群签名的各种安全要求，它的签名、验证和打开算法效率较高且签名长度较短。

参考文献

[1] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of ASIACRYPT'03. Berlin, Germany: Springer, 2003: 452-473.

[2] Zhang Guoyan, Wang Shaohui. A Certificateless Signature and Group Signature Schemes Against Malicious PKG[C]//Proc. of the 22nd IEEE International Conference on Advanced Information Networking and Applications. [S. l.]: AINA Press, 2008.

[3] Chaum D, Heyst V E. Group Signatures[C]//Proc. of EUROCRYPTP'91. Berlin, Germany: Springer, 1991: 257-265.

[4] Park S, Kim S, Won D. ID-based Group Signature[J]. Electronics Letters, 1997, 33(19): 1616-1617.

[5] Hu B, Wong Duanchuan, Zhang Zhefeng, et al. Key Replacement Attack Against a Generic Construction of Certificateless Signature[C]//Proc. of ACISP'06. Melbourne, Australia: [s. n.], 2006: 235-346.

[6] 陈　虎，宋如顺. 高效的无证书环签名方案[J]. 计算机工程，2009, 35(21): 125-127.

[7] Zhang Lei, Zhang Futai, Zhang Fangguo. New Efficient Certificateless Signature Scheme[C]//Proc. of EUC'07. Taipei, China: [s. n.], 2007: 692-703.

[8] 张　磊，张福泰. 一类无证书签名方案的构造方法[J]. 计算机学报，2009, 32(5): 940-945.

[9] 陈　虎，宋如顺. 无证书群签名方案[J]. 计算机工程，2009, 35(9): 130-132.

[10] Chen Xiaofeng, Zhang Fangguo, Kim K. A New Id-based Group Signature Scheme from Bilinear Pairings[EB/OL]. (2003-11-06). http://PPeprint.iacr.org/P2003P116.

编辑　陆燕菲

(上接第 17 页)

$$L(\boldsymbol{H},\boldsymbol{H}') = \sum_{b=1}^{B} H_b \ln H_b' \tag{8}$$

其中，$\boldsymbol{H}$ 和 $\boldsymbol{H}'$ 分别表示 2 幅纹理图像的特征向量，其特征维度为 B；H_b 和 H_b' 表示第 b 维特征占据所有特征的 比例。

文献[5]对比度的求解步骤为：在局部区域中，求得 P 个邻居像素点之间的方差，将其作为一个独立于 LBP 特征之外的 $\mathrm{VAR}_{P,R}$ 特征，并将 LBP 和 $\mathrm{VAR}_{P,R}$ 进行联合，共同表示纹理特征。在文献[5]的实验中，这种联合能够得到最佳的分类效果，所以将本文所提的 LMCP 方法所得实验结果与 LBP/VAR 方法所得结果进行比较。表 1 给出实验结果对比。

表 1　2 种方法在 Outex_TC_00012 数据上的正确分类率对比

P	R	L	LBP/VAR 方法/(%)			LMCP 方法/(%)		
			tl84	horizon	平均值	tl84	horizon	平均值
8	1	8	78.8	76.7	77.8	77.6	79.7	78.65
16	2	8	86.1	84.8	85.5	88.7	91.3	90.00
8/16	1/2	8	85.0	82.6	83.8	85.9	86.8	86.40

由于当 $L=8$ 时能够得到最佳实验结果，因此表 1 省略了 L 取值为非 8 的数据。从实验数据可以看出，当 $P=16$、$R=2$ 时，LMCP 的平均识别率为 90%，达到最佳；无论 P 和 R 取值为多少，LMCP 方法所得结果均优于 LBP/VAR 方法。

5　结束语

LBP 方法不能很好地反映局部像素间的对比度特征，即使联合 VAR 特征，也不能取得满意的结果。本文方法将局部像素间的对比度值相对于整个局部对比度值域区间的大小进行分层，得到的 LMCP 特征能够很好反映像素间对比度的相对大小，可以很好地减小不同光源和光照方向给纹理分类带来的非线性干扰。LMCP 特征具有光照不变性、旋转不变性、多分辨率等特征。实验结果验证了本文方法的正确性。

参考文献

[1] Mudigonda N R, Rangayyan R, Desautels J E L. Gradient and Texture Analysis for the Classification of Mammographic Masses[J]. IEEE Transactions on Medical Imaging, 2000, 19(10): 1032-1043.

[2] Harwood D, Ojala T, Pietikainen M, et al. Texture Classification by Center-symmetric Auto-correlation Using Kullback Discrimination of Distributions[J]. Pattern Recognition Letters, 1995, 16(1): 1-10.

[3] 赵银娣. 基于环形马尔可夫模型的纹理图像分类[J]. 计算机应用与软件, 2009, 26(12): 63-65.

[4] 宋余庆，刘　博，谢　军. 基于 Gabor 小波变换的医学图像纹理特征分类[J]. 计算机工程, 2010, 36(11): 200-202.

[5] Ojala T, Pietikainen M, Maenpaa T. Multiresolution Gray-scale and Rotation-invariant Texture Classification with Local Binary Patterns[J]. IEEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(7): 971-987.

[6] Ojala T, Maenpaa T, Pietikainen M, et al. Outex——A New Framework for Empirical Evaluation of Texture Analysis Algorithms[C]//Proc. of the 16th International Conference on Pattern Recognition. Quebec City, Canada: [s. n.], 2002: 701-706.

[7] Tan Xiaoyang, Triggs B. Enhanced Local Texture Feature Sets for Face Recognition Under Difficult Lighting Conditions[J]. IEEE Transactions on Image Processing, 2010, 19(6): 1635-1650.

编辑　陆燕菲