基于步态识别的移动设备身份认证模型

蒋 伟，王瑞锦*，余苏喆，秦圣智，李蝉娟，李冬芬

(电子科技大学信息与软件工程学院 成都 610054)

【摘要】智能移动设备遗失时，隐私泄露是一个大问题。现在的生物特征识别技术必须借助相应的辅助设备，如指纹识别、人脸识别等，认证操作复杂且成本较高。针对以上问题，该文提出一种基于步态识别的移动设备身份认证模型。在训练阶段，通过移动设备自带的加速度传感器对用户在日常生活中不同行为下的步态数据进行收集，提取特征形成特征向量并建立步态模型；在识别阶段，利用基于神经网络的模型匹配算法进行身份识别。系统实现采用C/S架构，所有传输数据采用国密SMS4对称加密算法进行加密，保证了数据传输的安全性。实验表明，神经网络算法的平均识别率为78.13%，综合反馈机制之后，可以达到98.96%的认证准确率。

关 键 词 步态识别； 身份认证； 智能移动设备； 对称加密

中图分类号 TN39 **文献标志码** A doi:10.3969/j.issn.1001-0548.2019.02.018

Research on Identity Authentication Model of Mobile Devices Based on Gait Recognition

JIANG Wei, WANG Rui-jin*, YU Su-zhe, QIN Sheng-zhi, LI Chan-juan, and LI Dong-fen

(School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract Privacy disclosure is a big problem when smart mobile devices lost. Now, the biometric technologies must rely on the corresponding auxiliary equipment, such as fingerprint recognition, face recognition, resulting in the authentication is complex and costly. To solve these problems, a gait biometrics-based mobile device authentication solution is proposed in this paper. In the training phase, the gait data of different behaviors of users in daily life are collected by the accelerometer in the mobile device. Then, the feature is extracted to construct feature vector and establish the gait model of users. The model matching algorithm based on the neural network is used to achieve the purpose of identification during the identification phase. The C/S architecture is applied to the implementation of the system. In order to ensure the security of network data transmission, all the transmission data is encrypted by SMS4 symmetric encryption algorithm. Lots of experiments show that the average recognition rate of neural network algorithm is 78.13 percent, and integrating the feedback mechanism, the authentication accuracy can up to 98.96 percent.

Key words gait recognition; identity authentication; smart mobile devices; symmetric encryption

随着智能手机的普及，智能手机的盗窃事件频发。据统计，2012年，美国约有160万部智能手机被盗。设备被盗后，隐私泄漏可能造成更大的危害。因而对于智能设备的防护技术变得日益重要。现有的安全软件大多是基于口令或手势等方式进行防护，但这种方式有一定的缺陷，如易仿制、易泄露、没有特异性、防护被动等。本文提出一种基于步态识别的移动设备身份认证模型，通过移动设备自带的传感器记录用户的步态特征，将其作为身份认证的标志，从而实现对移动设备的安全防护。通过步态特征实现智能移动设备对当前使用者的身份认证，以达到以下两个目的：1) 通过身份认证机制确定当前使用者或者携带者是否为合法用户，若非法则发送地理位置信息，以此来达到设备防盗的目的；2) 若确定当前用户或携带者非法，则锁定该移动设备，以此来达到合法使用者的隐私保护的目的。

收稿日期：2016－12－28；修回日期：2017－11－15

基金项目：国家自然科学基金(61472064, 61602096)；四川省科技计划(2018GZ0087, 2016FZ0002)；四川省教育厅重点项目(17ZA0322)；网络与数据安全四川省重点实验室开放课题(NDSMS201606)

作者简介：蒋伟(1982－)，男，博士生，主要从事移动数据管理及其应用、网络安全方面的研究.

通信作者：王瑞锦，Email: wrj8882003@163.com

1 相关研究

文献[1]通过计算机的动画来模拟和动态分析人体行走特征，具有基础的指导作用。文献[2]尝试用固定在身上的加速度传感器进行数据采集。这种方式能够收集到许多数据，并在多方面进行细致分析，但这种方式相对复杂，需要佩戴较多的传感器，实际使用效率不高。文献[3]基于部位检测的人体姿态识别，利用随机森林检测人体的31个部位，将人体的较小部位合并或把较小部位划分到相邻的主要部位中，用均值偏移算法获取各部位关节点的位置。该方法提高了低分辨率图像中人体关节点的平均预测准确率，可以识别人体姿态。文献[4]对人耳图像进行分析，提取人耳相关特征值(外耳轮廓点和耳型)，可以达到与其他生物识别技术相同的效果，并且可以弥补人脸识别、虹膜识别的不足，但该技术的识别率有待提高。文献[5]运用摄像头捕获人的行走图片，对大量捕获图片进行分析，建立相应的骨骼模型，实现对人的身份识别。这项技术可以应用在很多场合，但是，在捕获图像时需要摄像头等其他辅助设备显得有些不便。

上述研究表明，生物识别技术的研究日趋成熟且可以应用到实际生活中。目前基于步态识别的研究主要是对动作的识别[6-7]。本文基于运动步态识别技术[8]，利用移动智能设备自带的加速度传感器采集数据[9]，以步态特征为出发点，提出一种基于步态识别的移动设备身份认证模型。选择步态特征为认证关键，原因有3点：1) 步态识别技术可以在用户自然行走过程中进行主动识别，而脸部识别[10]、指纹识别[11]或瞳孔识别[12]则是被动等待用户去确认；2) 一个人的步态特征更加难以模仿，安全性有所增强；3) 移动设备自带的较为精确的传感器为识别技术提供了精准度上的支持。此外，本方案采用了移动设备自带的传感器进行数据收集，简单高效。

2 方案设计与系统实现

2.1 整体框架

本文提出的基于步态生物特征的移动设备身份认证系统的实现主要由客户端和服务端构成，包含3个子系统：1) 数据采集子系统：通过设备上的传感器采集用户的步态数据；2) 数据处理子系统：将收集得到的数据进行降噪处理，之后提取特征值，然后通过分类算法进行比较处理，得到最终结果[13]；3) 通知响应子系统：将数据处理所得到的结果通知反馈给用户。

智能移动设备作为客户端，运行数据采集子系统，一台服务器作为服务端，运行数据处理子系统和通知响应子系统。客户端通过网络和服务器通讯，使得3个子系统可以相互交换数据。

通过移动设备上的应用收集步态数据，计算特征值后通过互联网发送至指定的服务器。如果该数据是用于训练的，那么从数据中读取用户名和状态标签，加入数据库用来训练模型；如果该数据是用于识别的，那么从数据库读取并生成用户行为特征模型，识别用户行为，识别结束后，再从数据库中读取相应行为的数据并生成相应行为下的用户身份模型，识别用户身份。如果用户身份合法，则客户端应用正常工作；如果用户非法，通知客户端应用锁定移动设备，并立刻通知合法用户。整个身份认证分为两个阶段：训练和识别。

2.2 训练阶段

训练阶段需先选择训练模式，再由数据采集子系统采集数据后，通知数据处理子系统提取加速度传感器x、y、z 3个轴的数据进行数据的预处理，计算特征值，随后将计算出的数值运用神经网络、决策树等算法生成用户的步态模型，具体分为以下5个步骤。

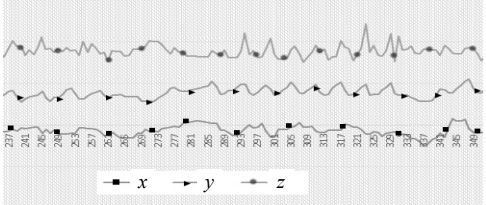
1) 训练模式选择

人在不同的运动状态下的步态特征是不同的，所以数据采集子系统应该为不同的运动状态打上不同的标签，标签来源于训练模式选择，在数据处理子系统建立步态模型阶段，根据不同的标签对同一个人建立不同的模型，因此，本文方案的身份识别率会大大提高。

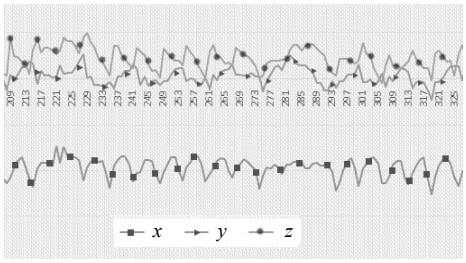
本文将收集的步态数据分为以下几种类型，即实现系统中可供选择的几种训练模式：走路、跑步、上楼梯、下楼梯和其他。

2) 数据采集

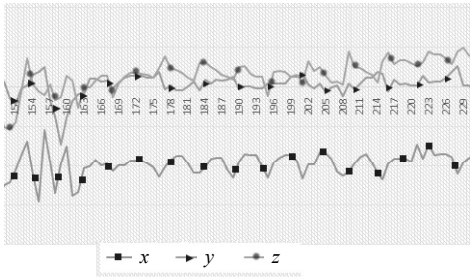
本文利用收集的移动设备中的加速度传感器数据(包括3个轴)变化体现用户在不同行为下的步态数据，图1为被测用户在走路时收集的步态数据。



a. 用户a步态数据



b. 用户*b*步态数据



c. 用户*c*步态数据

图1 用户走路时的步态数据

3) 数据预处理

对数据的处理包括时间窗口平滑、位置校准、滤波器过滤以及特征选择4部分，其中，时间窗口是对基础数据的基本操作，之后通过位置校准来重定位坐标系，再由滤波器进行进一步的降噪，最后得到该数据的特征值。

时间窗口设置为10 s，即一个时间窗口记录10 s的数据，即 $T_{\mathrm{A\_Win}}=10$。同时采用窗口重叠技术，本文使用50%的窗口重叠，即上一个时间窗口 C_i 记录进行至5 s时，下一个时间窗口 C_{i+1} 才开启，即 $T_{\mathrm{New\_Win}}=5$。对数据进行平滑时，选取当前的时间窗口 C_i、前一个时间窗口 C_{i-1} 和后一个时间窗口 C_{i+1}，取其平均值。

位置校准处理：由于用户摆放手机的方向有所差别，加速度传感器的竖直方向无法与重力加速度一致，导致传感器的数据产生误差，所以要进行位置的校准操作。当测试者静止时手机只会受到重力加速度的影响，但在实际情况下，各个方向都产生了加速度。可以假设*g*的方向与传感器的竖直方向夹角为α，*g*在传感器水平面上的投影与人体前进方向的夹角为β。在进行测量时传感器*x*、*y*、*z* 3个轴的数值为*A*，*B*，*C*，则真正的加速度值为：

$$A'=A\sin\beta-B\cos\beta+C\cos\beta$$

$$B'=B\sin\beta\sin\alpha-C\sin\beta\cos\alpha+C\cos\beta\sin\alpha$$

$$C'=B\sin\beta\cos\alpha+C\sin\beta\sin\alpha-C\cos\beta\cos\alpha$$

滤波器过滤：利用互补滤波器在三维空间内的走行方向投影到平面正交，再参照步态模型，在最大减速时间段平方处通过一个低通滤波器去除高频噪声与其他影响因素，最终将得到的向量通过中值滤波器，然后输出。

4) 特征提取

收集到的数据不能直观地体现出用户的步态特征，需要提取特征值来表达，比如峰值之间的时间(峰值间隔)可以体现出一个人正常的走路频率。本方案中需要提取以下特征值：平均值、标准差、平均绝对差、平均合成加速度、峰值间隔、离散化分布。假设有*n*条数据，3个轴为*x*轴，*y*轴，*z*轴，平均值为avg，标准差为sd，平均绝对差为aad，平均合成加速度为ara。

离散化分布：取出每个轴数据里的最大值和最小值，相减的差除以10的结果作为间隔，算出每个间隔里点的个数所占的百分比。

由图1可以看出，收集到的数据是不规则的，所以直接计算峰值间隔会有困难，本方案实现时采取拟合曲线来解决。

5) 建立模型

Weka作为一个公开的数据挖掘工作平台，集合了大量能承担数据挖掘任务的机器学习算法，包括对数据进行预处理、分类、回归、聚类、关联规则以及在新的交互式界面上的可视化。本文将收集到的所有数据，使用Weka建立用户状态模型，实验过程中分别运用了神经网络、朴素贝叶斯分类[14]、J48算法[15]和改进后的神经网络算法来建立模型，实验的结果表明改进后的神经网络效果最优。

本文采用经过改进的步态BP神经网络算法[16]。BP神经网络模型拓扑结构包括输入层(input)、隐层(hide layer)和输出层(output layer)。输入层神经元的个数由样本属性的维度决定，输出层神经元的个数由样本分类个数决定。隐藏层的层数和每层的神经元个数由用户指定。每一层包含若干个神经元，每个神经元包含一个阈值 θ_j 用来改变神经元的活性。前一层神经元和后一层神经元之间的权值为 w_{ij}，每个神经元都有输入和输出。输入层的输入和输出都是训练样本的属性值。O_i 是上一层的单元*i*的输出，而 θ_j 是单元*j*的阈值。神经网络中神经元的输出是由赋活函数计算得到的。该函数用符号表现单元代表的神经元活性。赋活函数一般使用Sigmoid函数或者Logistic函数。除此之外，神经网络中有一个学习率(*l*)，取值0～1，其有助于找到全局最小。如果学习率太小，学习将进行得很慢。如果学习率太大，可能在不适当的解之间摆动。

本文方案采用的算法伪代码如下：

fully_trained = FALSE;

DO UNTIL (fully_trained):

　　fully_trained = TRUE

　　FOR EACH

training_vector　$=< X_1, X_2, \cdots, X_n >$

FOR EACH J in hidden or output layer:

$$I_j = \sum_i w_{ij} O_i + \theta_j$$

FOR EACH J in output layer:

$$\mathrm{Err}_j = O_j(1-O_j)(T_j - O_j)$$

//计算误差

FOR EACH J in from last to first hidden layer:

$$\mathrm{Err}_j = O_j(1-O_j)\sum_k \mathrm{Err}_k w_{kj}$$

// k是j的下一层神经元

FOR EACH　w_{ij}　in network:

$$\Delta w_{ij} = (I)\mathrm{Err}_j O_i \quad // \text{ 权增值}$$

$$w_{ij} = w_{ij} + \Delta w_{ij} \quad // \text{ 权更新}$$

FOR EACH　θ_j　in network:

$$\Delta \theta_j = (I)\mathrm{Err}_j \quad // \text{ 偏差增值}$$

$$\theta_j = \theta_j + \Delta \theta_j \quad // \text{ 偏差更新}$$

　　IF (fully_trained):

　　　　BREAK

2.3　识别阶段

在识别阶段，数据采集子系统实时采集加速度传感器的数据并让数据处理子系统通过训练阶段生成的用户步态模型进行匹配处理，识别出当前用户是否合法，如果用户非法，则触发通知响应子系统做出相应处理。

2.3.1　收集待识别用户数据

该步骤与训练阶段的数据采集类似，不同的是，该步骤所收集到的数据是没有标签和姓名的，仅有x、y、z 3个轴的数据。

2.3.2　模型匹配

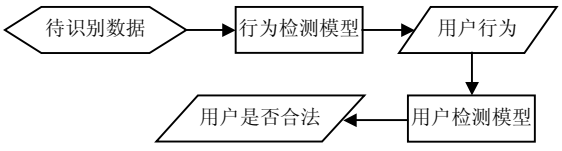


图2　模型匹配流程图

获取到数据后，进行特征提取，将提取出来的特征作为模型的输入，得到识别结果。结果是走路、跑步、上下楼梯和其他4种状态中的一种。然后，将数据与用户步态模型进行匹配，即可得到产生该数据的用户是否合法，并将分析结果传递给下一阶段。模型匹配流程图如图2所示。

2.3.3　通知响应

从模型匹配中获取用户是否合法，分为两种响应机制：

1) 若用户合法，不做响应；

2) 若用户非法，服务器会锁定客户端设备，随机生成6位验证码，利用用户的密码生成加密密钥，用该密钥对验证码进行加密，通过邮件和短信两种方式发送加密后的验证码。合法用户收到密文后在服务器web页面输入使用的密码即可解密得到验证码。通知响应系统流程图如图3所示。

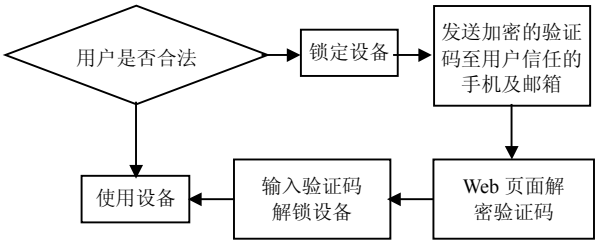


图3　通知相应系统流程图

3　安全性分析

3.1　设备安全性

本文认证系统旨在保证设备的使用安全性，合法用户在使用设备时，一切正常。非法用户(除机主以外的任何用户)试图使用设备时，服务器会立即将设备锁定，并发送加密的验证码到合法用户信任的手机号码和邮件，只有知道解密密钥或在机主的帮助才可以继续使用设备，保证设备在可控的安全范围内使用。一旦设备被陌生人使用，极有可能是设备被盗，机主可以在一定时间内进入服务器web页面，远程控制、锁定或定位设备，有助于设备的找回。

3.2　数据传输安全性

为保证身份认证系统中涉及的客户端和服务器二者传输数据的安全性，所有经过网络传输的数据都是经过国密SMS4对称加密算法加密的，保证了数据的安全性与机密性。该算法的分组长度为128 bit，密钥长度为128 bit。加密算法与密钥扩展算法都采用32轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

3.3　远程控制安全性

当用户想要使用远程控制功能时，可以登录到服务器，输入自己的账号和密码，选择将要执行的控制命令，如震动、通报地理位置、销毁文件等，

服务器会根据用户名和密码以及当前的时间生成一个远程命令代码，用户只要在一定时间内将代码发送至目标手机，即可完成对应的远程控制，若超出规定时间，命令失效，由此可以防止重复攻击。

3.4 通知响应安全性

若数据处理系统分析出用户非法，则会锁定目标设备，并向用户注册软件时填写的信任邮箱和手机号码发送验证码，验证码是经过用户使用的密钥加密的，合法用户在web输入其使用的密码，解密得到验证码，解锁设备。

4 测试结果

本文方案的客户端以安卓应用形式实现，结果测试在Android4.0.4版本手机上进行，手机硬件参数如表1所示。

表1 测试手机硬件参数

参数名称	参数值
CPU	高通骁龙Snapdragon MSM8260、1.5 GHz
GPU型号	高通Adreno220
RAM/GB	1
ROM/GB	4
扩展容量/GB	16
电池	可拆卸、1 930 mAh

4.1 训练测试

走路训练客户端显示界面及服务器的响应如图4所示。

a. 客户端运行图

b. 服务器端运行图

图4 走路训练测试结果

4.2 识别测试

识别测试仅展示识别非法结果，客户端界面与服务器响应系统的通知如图5所示。

a. 客户端锁定界面

b. 服务器响应通知

图5 识别非法测试结果

4.3 系统识别率

系统识别率是评判各种身份认证方案系统的重要指标。用户识别正确率(识别率)为：

识别率=(正确识别次数/总次数)×100%

经过大量的系统测试，系统识别86.7%的用户为合法用户，其余为非法用户。

从图6可以看出，对于同一用户来说，不同行为时的识别率也有所不同。用户在走路时，系统的识别率可达85.79%，并且十分稳定；用户在跑步时，识别率可达83.70%，上下楼梯时，略有差异，但都可达80%以上；由于其他类型行为的步态特征不是很明显，相比之下，系统识别率显得较低。

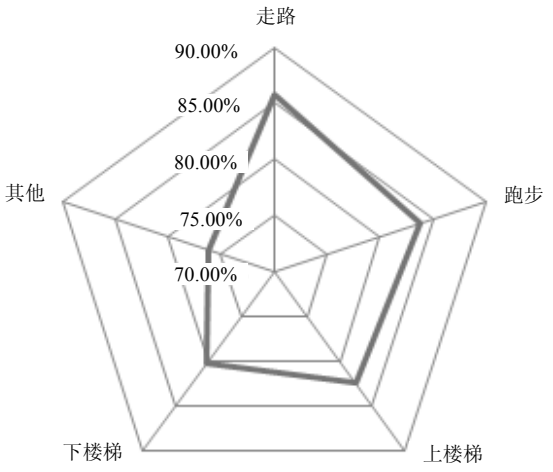


图6 同一用户不同行为的识别情况

本文对不同训练次数下用户整体的识别率做了

测试，如图7所示。可以看出，不同用户的识别率都在70%以上，并且随着训练次数的增加，所有用户的合法性识别都有一定程度的增加，训练5次的识别率可以达到80%左右，甚至90%。

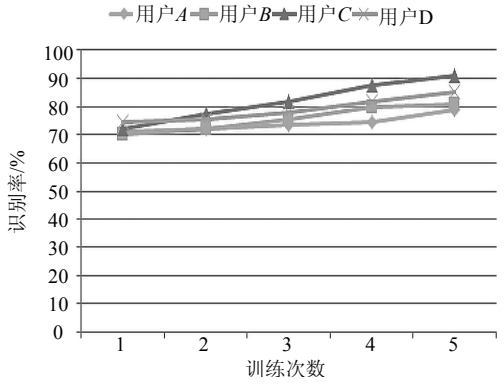


图7　不同用户不同训练次数下的识别情况

5　结 束 语

本文基于智能移动设备内置的加速度传感器，提出了基于步态生物特征的身份认证系统，该系统通过数据的收集、特征的提取和模型的匹配实现身份识别。与其他生物特征相比，步态具有提取简单、不易模仿等优点。本文方案认证便捷、方法独特、控制简单。

对于数据收集，本文方案仅仅用到了智能移动设备中的一个加速度传感器，因此识别的效率可能不是很高。使用多个传感器进行数据的采集以及采用量子计算和量子通信技术[9-14]，由此来提高系统的准确率将是未来的研究方向之一。

参 考 文 献

[1] FAURE F, DEBUNNE G, CANI-GASCUEL M P, et al. Dynamic analysis of human walking[C]//Proceedings of the Eurographics Workshop. Budapest: [s.n.], 1997: 53-65.

[2] MANTYJARVI J, LINDHOLM M, VILDJIOUNAITE E, et al. Identifying users of portable devices from gait pattern with accelerometers[J]. IEEE International Conference on Acoustics, 2005, 2(2): 973-976.

[3] 殷海艳, 刘波. 基于部位检测的人体姿态识别[J]. 计算机工程与设计, 2013, 34(10): 3540-3544.
YIN Hai-yan, LIU Bo. Recognition of human pose based on position detection[J]. Computer Engineering and Design, 2013, 34(10): 3540- 3544.

[4] 袁立, 穆志纯, 徐正光, 等. 基于人耳生物特征的身份识别[J]. 模式识别与人工智能, 2005, 18(3): 56-61.
YUAN Li, MU Zhi-chun, XU Zheng-guang, et al. Identity recognition based on human ear biometrics[J]. Pattern Recognition and Artificial Intelligence, 2005, 18(3): 56-61.

[5] ROHAN B, ANIRUDDHA S, KINGSHUK C. Gait based people identification system using multiple switching kinects[C]//International Conference on Intelligent Systems Design & Applications. [S.l.]: IEEE, 2013: 182-187.

[6] 姜鸣, 王哲龙, 刘晓博, 等. 基于BSN和CHMMs的人体日常动作识别方法研究[J]. 大连理工大学学报, 2013, 53(1): 121-126.
JIANG Ming, WANG Zhe-long, LIU Xiao-bo, et a1. Research on human daily activity recognition method based on BSN and CHMMs[J]. Journal of Dalian University of Technology, 2013, 53(1): 121-126.

[7] UGULINO W, CARDADOR D, VEGA K, et a1. Wearable computing: Accelerometers' data classification of body postures and movements[M]. [S.l.]: Springer, 2012, 7(2): 52-61.

[8] 张君宽. 基于BP神经网络步态识别的研究[J]. 中国安防, 2016(Z1): 99-101.
ZHANG Jun-kuan. Research on BP neural network gait recognition[J]. China Security, 2016(Z1): 99-101.

[9] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li, et al. Quantum information splitting of arbitrary two-qubit state by using four-qubit cluster state and Bell-state[J]. Quantum Information Processing, 2015, 14(3): 1103-1116.

[10] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li, et al. Quantum information splitting of arbitrary three-qubit state by using seven-qubit entangled state[J]. International Journal of Theoretical Physics, 2015, 54(6): 2068-2075.

[11] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li. Quantum information splitting of a two-qubit Bell state using a four-qubit entangled state[J]. Chinese Physical C, 2015, 39(4): 26-30.

[12] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li. Quantum information splitting of arbitrary three-qubit state by using four-qubit cluster state and GHZ-state[J]. International Journal of Theoretical Physics, 2015, 54(4): 1142-1153.

[13] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li, et al. Quantum information splitting of arbitrary three-qubit state by using seven-qubit entangled state[J]. International Journal of Theoretical Physics, 2015, 54(6): 2068-2075.

[14] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li, et al. Splitting unknown qubit state using five-qubit entangled state[J]. International Journal of Theoretical Physics, 2016, 55(4): 1962-1972.

编　辑　叶　芳