第38卷 第21期
Vol.38 No.21

计 算 机 工 程
Computer Engineering

2012年11月
November 2012

• 安全技术 •

文章编号：1000—3428(2012)21—0133—05 文献标识码：A 中图分类号：TP391

异源码字信息无序交融机制及其应用

周 珂，戴 永，樊 亮

(湘潭大学智能计算与信息处理教育部重点实验室，湖南 湘潭 411105)

摘 要：目前利用单模态密码进行身份认证存在输入方式单一、安全性低等缺点。为此，提出一种异源码字可无序交融输入的方法。建立异类模态密码码字产生硬件的融合机制，给出异类模态密码码字信息归一化格式，为不同的模态信息设计不同的前置处理和密码码字分类等算法，通过异源码字公共单元实现异类模态密码码字的无序交融。基于密码键盘与黑箱子指书2类模态码字的无序交融应用实例表明，该机制可以较好地用于多模态密码输入系统。

关键词：多模态密码输入系统；异源码字；无序交融；密码键盘；黑箱子指书盘

Disordered Fusion Mechanism of Heterologic Code Word Information and Its Application

ZHOU Ke, DAI Yong, FAN Liang

(Key Laboratory of Intelligent Computing and Information Processing of Ministry of Education, Xiangtan University, Xiangtan 411105, China)

【Abstract】Single-mode password authentication has kinds of disadvantages, like single input mode and low security. This paper proposes a method to disordered fusion input for heterologic code. It builds fusion mechanism based on hardware generating of heterologic model code, gives normalized form of heterologic model code information, and designs the corresponding algorithm, like different pre-processing and classification of password code, for different model information. Disordered fusion of heterogeneous model code is implemented through public unit of heterologic code. Application of disordered fusion based on password keyboard model and black box model show that the mechanism is suitable for multi-mode password input system.

【Key words】multi-mode password input system; heterologic code word; disordered fusion; password keyboard; black box keyboard

DOI: 10.3969/j.issn.1000-3428.2012.21.036

1 概述

来源于不同模式形态的密码码字称为异源码字或多模态码字，反之称为同源码字或单模态码字。迄今，诸如金融交易、权限工作等系统一直沿用单模态密码进行身份认证，尤以密码键盘使用普及。密码键盘在密码交互中以其输入方便、保密性好、体积小、成本低、寿命长等优势成为社会活动中的普及型身份认证方式。由于客户指纹、脸面、虹膜等人体生物信息特征具有不一致性、唯一性、时限性等重要属性，因此这些生物特征信息识别系统无法替代密码键盘在金融交易系统中的存在。但在长期使用过程中，密码键盘的安全性、可靠性等受到严峻挑战，用户密码被肩窥事件时有发生；因用户指击导致操作结构损毁严重，常常出现密码因硬件问题输入出错的情况。针对指击密码键盘的不足而产生的图形密码[1-2]及各种手写密码输入方法与装置[3-5]虽然对部分肩窥行为如偷看、听音、有光摄像等有较好的预防作用，设备寿命也有所延长，但由于仍局限于单模态操作因此无法从根本上摆脱相应摄像方法的偷窥，单模态手写密码输入方法更是无法回避误识率。为解决上述以密码键盘作为客户身份认证面临的问题，本文提出异源码字信息可无序交融输入的身份认证机制，该机制的特点主要表现在：(1)异类模态的硬件操作无序性；(2)异类模态使用的随意性；(3)异类模态码字模式分类信息的交融性；(4)异类模态密码码字排序结构的传统性；(5)异类模态码字信息产生方式的互补性。

2 多模态密码输入系统体系结构

图1为本文多模态密码输入系统的体系结构。该体系结构的工作环节分属3种系统：模态信息实时获取由模态感知器系统完成；N模态原始信息结构规范化处理与传送由直接计算机系统完成；上位机完成N模态信息前置处理与结构还原及N模态功能代码与密码码字识别等。

基金项目：湖南省高校创新平台开放基金资助项目(09K040)；湖南省“十二五”重点学科建设基金资助项目

作者简介：周 珂(1987－)，男，硕士研究生，主研方向：模式识别；戴 永，教授；樊 亮，硕士研究生

收稿日期：2011-12-30 **修回日期：**2012-02-28 **E-mail：**kusheng176@hotmail.com

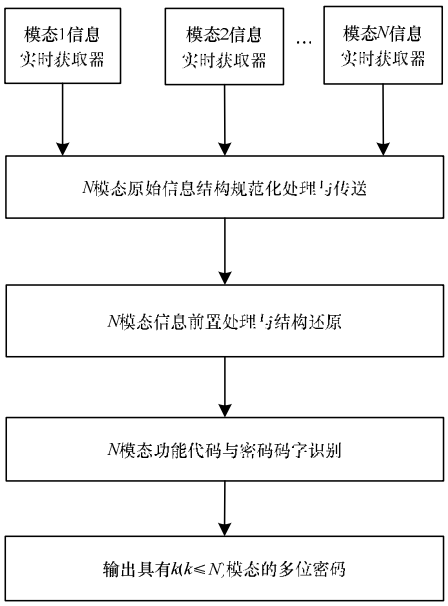

图 1 多模态密码输入系统体系结构

本文机制接纳 N 种模态码字信息。为满足模态信息无序交融的工作要求，感知信息源不设优先级，只注重模态信息发出的先后顺序[6]。由模态信息感知系统发出的模态原始信息被直接计算机接收，并进行结构规范化处理，处理结果以双机通信的方法送至上位机。

N 种模态建立 N 种模态信息前置处理模块集。前置处理的内容根据模态属性而定，基本目标是实现相应模态码字的不变结构信息的还原。

来自于前置处理环节的异源码字信息的实义内容分为 2 类：一类是功能信息，即当前的模态信息是让系统完成某项对应功能；另一类是数码信息。模态信息分类由 N 模态功能代码和密码码字识别、输出具有 $k(k\leqslant N)$模态的代码码链 2 个环节完成。

3 异源码字信息综合

设任意模态感知器提供的模态信息所占据的最大字节数已知，N 种模态有 N 个最大字节数，取 N 个最大字节数中最大值 $BUFMAX$，按该值建立多模态原始数据缓冲区。缓冲区存放 2 个字段，第 1 个字段为模态统一编号，占一个字节；第 2 个字段为模态原始信息字段，字节数为 $BUFMAX$。直接计算机与上位机的传输协议除帧、波特率外，上位机串口通信的激活字节数为 $BUFMAX$+1。

当上位机接收到直接计算机提供的具有规范格式的模态感知器信息后，依据规范格式模态信息第 1 个字节提供的模态编号进入相应的模态信息处理分支，进行原始模态信息的前置处理与模式识别，集成算法流程如图 2 所示。其中，MM 为多模态有效信息公共存放单元，当前模态的模式被识别后，相应符号编码送入 MM。MM 中的代码完全脱离了模态影响而成为纯粹的数字符号代码。

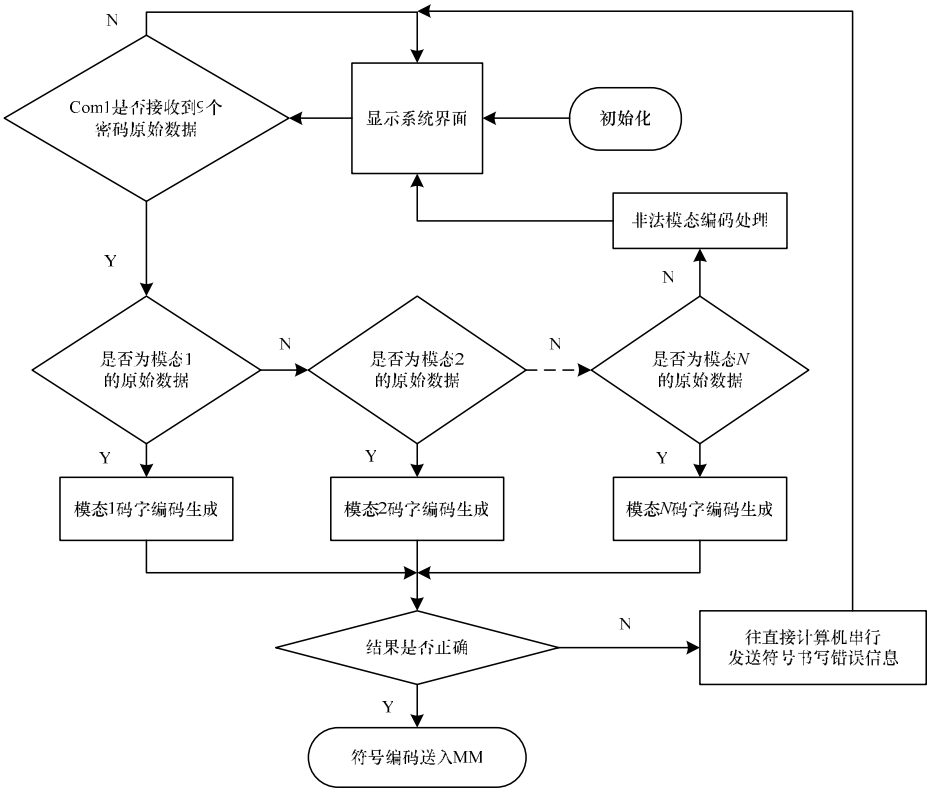

图 2 模态信息处理流程

当前 MM 提供的数字符号代码是单一模态的单一符号代码，通常包含 2 种含义：一种为单符号的功能代码，对于功能符号，系统进入相应的功能模块运行；另一种是位数据码，位数据码需和已输入的数据码链进行后缀拼接，直至拼接长度达到规定的数据码位长度，才能将该符号链进行整体输出。代码综合算法流程如图 3 所示。上游模块接收到的符号链可作为组合符号功能代码，也可作为限位数据或某种意义的编码等应用。

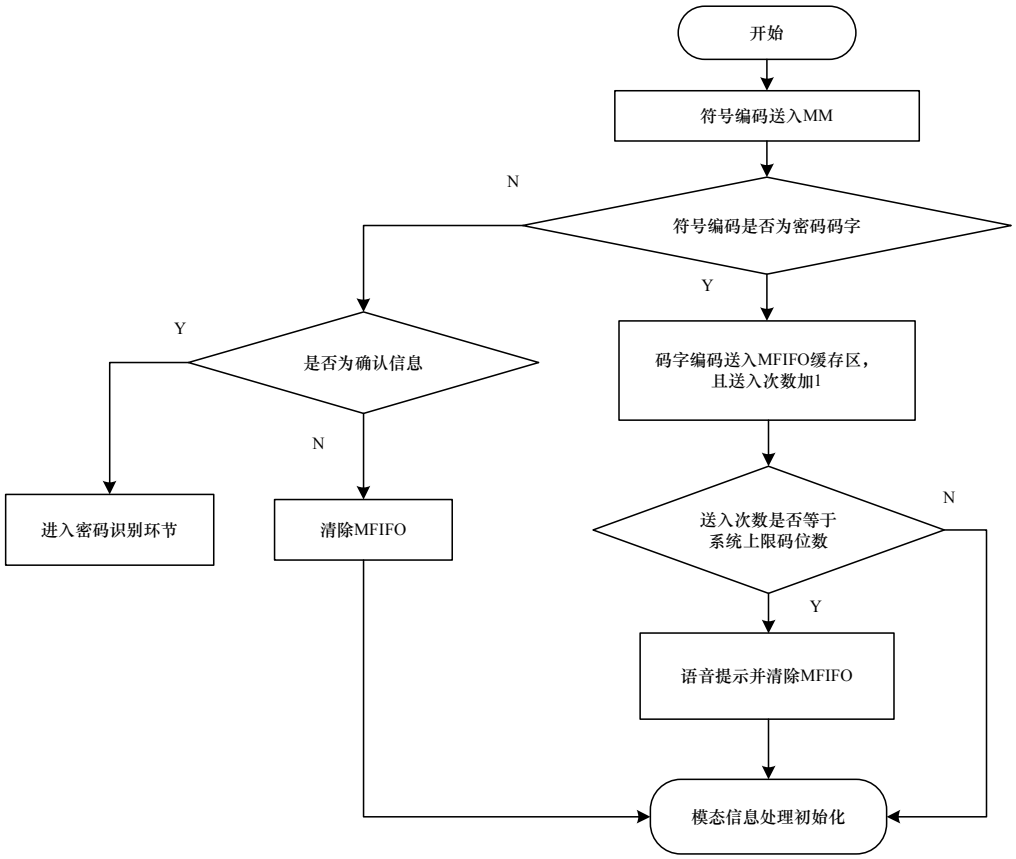

图 3 码字属性区分流程

4 应用系统实例

本文基于异源码字信息无序交融机制，设计了一个异源码字可无序交融提供密码的密码输入系统。系统的硬件结构如图 4 所示，主要模块包括密码键盘 JP、黑箱子指书密码书写盘 ZP、单片微型计算机 IC1、语音模块 IC5、串口通信模块 IC3 及 PC 等，系统取 N=2，$BUFMAX$+1=9，单符号功能码，密码长度为 6 位，IC1 采用 89S51，IC2 为 8255，IC3 为 MAX232。

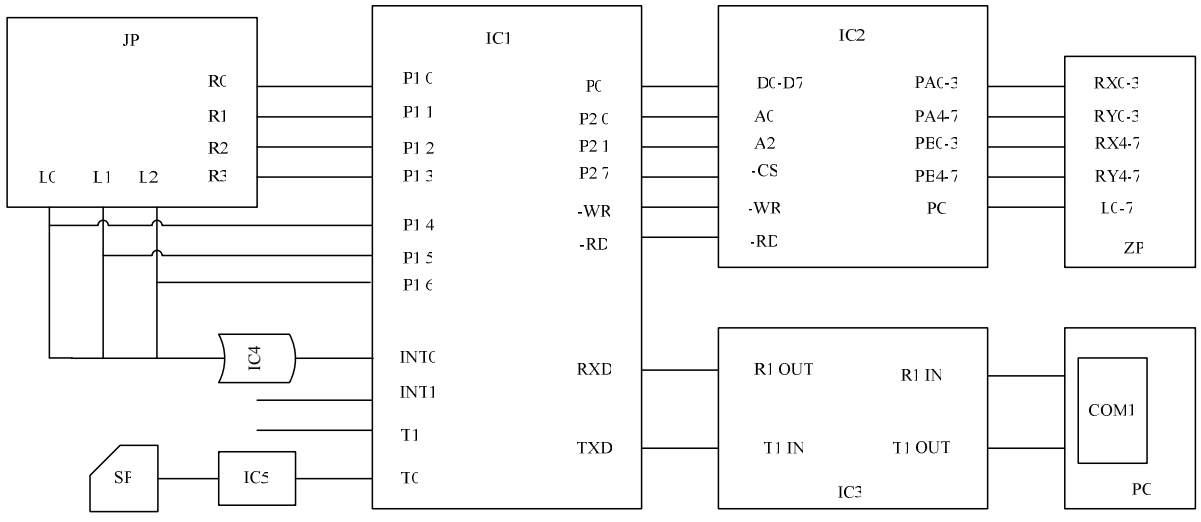

图 4 系统硬件结构

4.1 感知器结构

感知器包括以下 3 个部分：

(1)密码键盘模态感知

密码键盘模态感知结构由密码键盘主结构模块 JP 及辅助逻辑电路 IC4 组成，电路连接与现有的密码键盘大同小异。

(2)黑箱子密码指书盘模态感知

黑箱子密码指书盘模态感知系统由指书模块 ZP 和 IC2 组成，ZP 为具有 32×32 像素、可书写面积为 100 m×100 m 的红外触摸书写盘，它利用 x、y 方向上密布的红外线矩阵来检测并定位用户的触摸，IC2 为外部扩展的 I/O 口，用作采集并向 IC1 传送 ZP 所采样的数据。IC2 中 PC

通道提供 8 组驱动信号，每位信号分别对应 x 方向和 y 方向的 4 对红外对管信号，通过 PA、PB 通道获取到的感知信息反馈到主系统中。8 组完全驱动一次为一帧图像数据，通过对红外矩阵不间断地扫描获取书写者的全部书写信息。为实现书写时只须“心-指”关联，本文系统将 0~9 10 个密码符号及“确认”、“清除”2 个功能符号均设置为可一笔写成的符号，重新定义书写结构的符号：

1)“4”用“φ”代替，“5”用“S”代替，“确认”改为“∨”，相当于打钩；

2)“清除”改为“∧”，相当于重新输入。

(3)密码模态感知结构扩展

缺省模态可通过 IC1 中的 INT1 进行扩展，可扩展的模态有语音、手语。以中断、查询、中断查询相结合、中断与无条件扫描以及其他方式来进行信息交互。

4.2 密码获取

密码键盘码字获取方法为传统方法，本节重点讨论指书密码码字的获取原理。设 V_{max} 为人们的最快指书速度，$d_{i\text{-}1,i}$ 为指书过程中任意前后被采集的两点的距离，$t_{min}(d_{i\text{-}1,i})$ 为两点的最短时间，即 $t_{min}(d_{i\text{-}1,i})=d_{i\text{-}1,i}/V_{max}$。本文系统取 $t_{min}(d_{i\text{-}1,i})$=2 ms。

由于指书模块密码输入者采用指书模态进行密码输入时，书写的笔迹速度具有不确定性，导致上位机所采样到的笔迹点比较稀疏，无法完整或较好地反映出所书写的原始轨迹，因此必须对获取的数据点进行插值处理，来重构书写的原始轨迹，从而便于后续的数据处理与分析。

图 5 为码字“4”的指书信息获取结果的点阵显示。

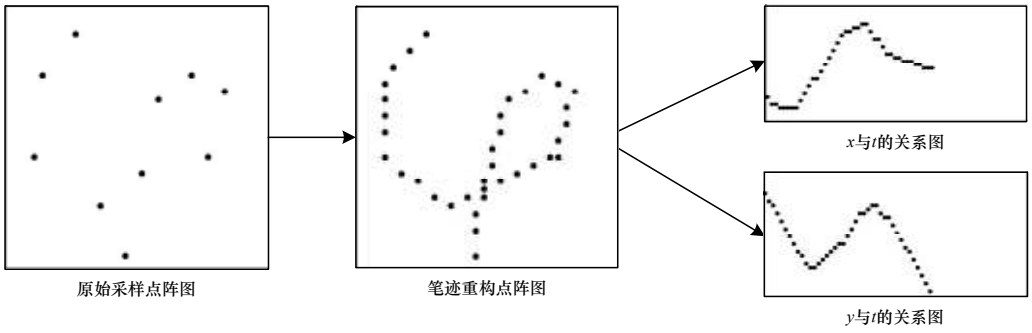

图 5 “4”的指书信息获取示例

以关键点和分量时序作为指书符号特征。关键点主要包括起点、终点、拐点等。关键点抽取算法如下，其中，P_{in} 表示采样点序列；P_{out} 表示关键点序列。

算法 1 关键点抽取

输入 采样点序列 $P_{in}=\{p_i:(x_i,y_i),(i=1,2,\cdots,m)\}$

输出 关键点序列 $P_{out}=\{p_j^{'}:(x_j,y_j),(j=1,2,\cdots,l)\}$

```
void KeyPoint(int startIndex, int endIndex)
{const double DISTANCE = 2.0;   //设定距离的阈值
 double maxDistance = 0.0;   //所求点到直线最大距离存放空间
 double distance = 0.0;   //所求点到直线距离存放空间
 int maxPosition = 0;
 int length = P_in.size();   //容器长度
 for(int i=startIndex+1;i<endIndex;i++)
 { double x0 = IntToDouble(P_in[i].x);
 double y0 = IntToDouble(P_in [i].y);
 distance = PointToLineDistance(x0,y0,x1,y1,x2,y2);
//计算点(x0,y0)到经过(x1,y1)、(x2,y2)两点直线的距离
 if(maxDistance < distance)
//获取所求距离中最大的存入 maxDistance
 {maxDistance = distance;
  maxPosition = i; }//end if      }      //end for
 if (maxDistance >= DISTANCE)
 { P_out.push_back(maxPosition); //将抽取的关键点存入 Pout
KeyPoint(startIndex,maxPosition);
//进行笔段分割，继续进行关键点抽取
  KeyPoint(maxPosition,endIndex);}
 //end
```

基于手写数字与采样时间之间的关系，把传统的二维向量信息转换为与采样时间相关的三维向量信息：

$$\boldsymbol{f}_1(x_i,y_i)\Rightarrow \boldsymbol{f}_2(x_i,y_i,t_i),i\in[0,n]$$

其中，n 为采样数据点总量。

然后进行如图 5 所示的 x、y 分量时序分解：

$$\boldsymbol{f}_2(x_i,y_i,t_i)\Rightarrow \boldsymbol{f}_3(x_i,t_i)\cup \boldsymbol{f}_4(y_i,t_i)$$

对应于 x、y 分量时序结构的特征有 x 方向和 y 方向上的极值以及极值间在时间 t 上的关系。

针对 $\boldsymbol{f}_3$ 和 $\boldsymbol{f}_4$ 二次曲线的不变性进行分析而获取 x、y 分量时序特征的算法如下，其中，*vector* 为存放时序特征向量的容器。

算法 2 分量时序特征抽取

输入 采样数据集合 *Cpoint Data*

输出 时序特征向量

(1)将采样数据进行时序分解：

```
for ( j=0;j<Data.sizeof(); j++ )
//将二维坐标分解为 x 方向和 y 方向 2 个序列
{ Datax[j] = Data[j].x;
 Datay[j] = Data[j].y; }
```

(2)判断笔画的起笔方向，存入 *vector*。

(3)分别计算 x、y 方向上的极点信息以及与时间 t 的

关系，存入分量时序特征容器 *vector*。

(4)计算字符的重心，存入分量时序特征容器 *vector*。

(5)判断时序特征是否完全，如果是，则结束；否则，转步骤(2)。

以关键点作为初分类特征，分量时序作为二次细分类特征。利用支持向量机进行手写体数字识别，输入层就是经过前置处理和特征提取所获取的规范化分类特征向量，输出是若干中间层节点的线性组合，而每一个中间层节点对应于输入样本与一个支持向量的内积，支持向量的具体数目由训练过程得到，因此，也称为支持向量网络[7]。

指书符号的高要求为[6 cm, 10 cm)，除“1”外，其他符号的宽须大于 4 cm。

将来自于密码键盘和指书盘的密码码字按图 2、图 3 中的相关环节进行处理，得到用户输入的密码或完成功能操作。

5 异源码字密码结构实验与安全性分析

对于确认的 M 位密码中的每一位，分别采用 N 种模态输入，最大的输入密码码字结构数为 $10^M C_M^{N\times M}$，一条给定密码的模态结构数为 N^M。取 M=6，N=2，密码数量为 $10^6 C_6^{2\times 6}$，窃取率为 $1/10^6 C_6^{2\times 6}$。

以“123456”6 位为实验密码，相应的密码结构输入实验与安全性分析如图 6 所示。从中可以看出，使用同源码字进行密码输入时，虽然工作效果没有本质上的区别，但是其安全性存在很大的隐患，键盘模态进行密码输入容易被他人窥视，指书模态则容易被摄像密码输入过程。双模态交融输入方式的安全隐患仅存于双模态时序同步摄像肩窥，而且黑箱子内必须是无光源摄像。同样，$N(N>1)$ 模态交融输入方式的安全隐患仅存于 N 模态时序同步肩窥。可见，对 N 模态交融输入方式进行肩窥所需的设备成本、密码重构技术等是目前所有密码肩窥行为中最高的。

输入符号	键盘模态	指书模态	键盘、指书双模态交融					
			单手输入				双手输入	
			示例 1		示例 2		左手键盘	右手写盘
			键盘	写盘	键盘	写盘		
1	①	1	①		①			1
2	②	2		2		2	②	
3	③	3	③			3	③	
4	④	φ		φ		φ		φ
5	⑤	S	⑤		⑤			S
6	⑥	6		6	⑥		⑥	
确认	确认	∨	确认		∨		∨	
缺陷	没有码字结构错误	存在码字信息误识率	存在码字信息误识率				存在码字信息误识率	
安全隐患	窥视	摄像	窥视与摄像同步进行				窥视与摄像同步进行	

图 6 密码输入的安全性分析

6 结束语

为提高金融交易系统密码码字输入过程的防肩窥能力和水平，在硬件上采用多模态感知结构具有密码输入形态的多样性、使用更为便捷、提高肩窥设备成本和技术要求、可靠性更高、系统使用寿命更长等优点。与现有方法相比，本文方法的硬件成本仅为黑箱子指书密码盘，实际使用结果表明，软件的复杂程度及其带来的开销未给用户带来不适感觉。

参考文献

[1] Birget J C, Hong Dawei, Memon N. Graphical Passwords Based on Robust Discretization[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(3): 395-399.

[2] 胡 卫, 马常楼, 廖 巍. 图形密码方案可用性及安全性分析[J]. 计算机应用与软件, 2010, 27(12): 55-57.

[3] 郑召生. 防窥视用密码输入装置: 中国, 200720022085[P]. 2008-04-09.

[4] 戴 永, 王求真. 联网门禁系统的资源节约与人性化技术研究[J]. 湘潭大学自然科学学报, 2008, 30(2): 81-84.

[5] 肖启冉. 防窥视触摸式密码输入键盘: 中国, 200720040387[P]. 2008-06-04.

[6] 于 浩, 朱志勇, 蒋朝惠. 传感器网络中连通覆盖算法研究[J]. 湘潭大学自然科学学报, 2009, 31(3): 148-153.

[7] 戴 永, 曾艳艳. 基于 RBF 神经网络的手绘电气草图分类研究[J]. 湘潭大学自然科学学报, 2010, 32(4): 102-107.

编辑 张 帆