基于 Android 行为的加密应用系统研究

姜春风

（吉林农业科技学院 信息工程学院，吉林 吉林 132101）

摘　要：随着手机的广泛使用，其安全性也逐步被人们所认识，用字母数字组合的传统加密方式繁琐且易被伪造。本文采用行为加密的方式，通过移动设备识别加密者的行为，对移动设备进行加密，以保证移动设备中资料的安全。并且在 Google 开发的 android 手机平台上，设计了针对移动平台的行为加密应用系统，实现了行为加密算法，并验证了本文给出的行为加密应用系统的有效性和可行性。

关键词：Android；行为加密；安全；应用

中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1008-8725(2010)09-0159-03

Research on Action-based Encryption Application System Based on Android

JIANG Chun-feng

(School Information Engineering, Jilin Agricultural Science and Technology College, Jilin 132101, China)

Abstract: Security of mobile platform has been recognized with the widespread use of mobile phones. Traditional Encryption styles, combined with alphabets and numbers, are miscellaneous and can be easily forged. This paper proposes a new algorithm called action-based encryption, identifies actions to encrypt on mobile platform and to assure the safety of mobile platform information. With the android exploited by google, action-based encryption application system has been designed and realized focusing on the mobile platform. Finally, validity and feasibility of this system has been demonstrated on a mobile platform.

Key words: android; action-based encryption; security; application

0　引言

移动终端的广泛使用及其日益增加的功能带来了新的安全问题，为了保护用户的信息安全，需要了解并解决这些安全性问题。因此，移动平台信息的加密解密已成为研究的热点。在传统加密解密系统中，多数采用字母数字组合的键盘输入方式，但是在使用频率较高的移动平台上，反复使用高强度密码进行加密解密比较繁琐。因而需要设计出一种方便快捷的行为加密算法，即通过验证使用者对手机的一个动作行为，判断使用者是否合法。

1　Android

Android 是一个开放性移动设备综合平台，它是一个针对移动设备的程序集，其中包括一个操作系统，一个中间件和一些关键性应用。其中媒体方面对一些通用的 audio, video, 和图片格式提供支持。Google 发布了它的移动平台操作系统 Android SDK 开发环境，包括：一个设备模拟器，调适工具，内存和效率调优工具和一个 Eclipse 的插件等。这款模拟器功能非常齐全，用户可以使用键盘输入，鼠标点击模拟器按键输入，还可以使用鼠标点击、拖动屏幕进行操纵。其主屏分辨率达 320*480 像素，彩屏。所以本文选择这款模拟器作为开发环境。

2　行为加密算法设计

2.1　行为

行为是有机体在外界环境刺激下引起的反应，包括内在的生理和心理变化。人的行为由 5 个基本要素构成，即行为主体、行为客体、行为环境、行为手段和行为结果。本文所讨论的行为特指使用者针对移动平台作用的生理行为。针对移动平台的行为有很多，如：以一定频率翻转手机，抛动手机等等。但是这些行为显然需要硬件设备的支持，而普通的移动平台一般不会配备这些设备。上述行为不作为本文的研究对象。由于 android 手机操作系统提供了触摸屏环境，在其 GPhone 模拟器上设计行为加解密系统，可以狭义限定这里讨论的行为是指针对手机屏幕的行为，即在触摸屏上的一系列操作组合。也就是说这里的研究对象是时间和空间的有机结合。

2.2　存储用户的行为

首先是空间的存储。这里所说的空间就是在触摸屏的环境下画图形，通过图形的比对作为整个行为加密解密匹配的一部分。为了加密解密便捷，可以认为用户输入图形中每个像素只有着色和未着色 2 种情况，所以可以直接将原始图形二值化，将原来的图形信息保存在一个与屏幕像素相等的矩阵（320*480）中，并初始化所有矩阵元素为零，而后笔迹划过的像素点在矩阵中对应单元的值置 1。这样就把用户输入的图形转换为矩阵形式，方便后面的处理。

其次是时间的存储。在存储图形基础上，同时记录下用户输入的轨迹，这样时空结合，就能准确的描述一个针对移

动平台的行为。在触摸屏上的动作一共只有 3 种，即落笔、拖动、抬笔。无论用户的这个行为多么复杂，总是上述 3 个步骤的循环。在移动平台上，可以通过函数调用存取时间，所以这个方法是可行的。当用户键入加密解密行为时，采用表 1 的数据结构保存轨迹。

表 1　轨迹元素数据结构

指针 P	落笔坐标 (x_1,y_1)	抬笔坐标 (x_2,y_2)	消逝时间 (以秒为单位)

用户在开始划出第一笔的时候，分配一个内存单元，将 head 指针指向刚分配的单元。并通过函数获得落笔时刻的坐标信息和时间信息，在用户抬笔时刻再次获得抬笔坐标和时间信息。两次时间相减，即为消逝时间。如果用户再次落笔，则再次分配内存单元，且将指针 p 指向新的单元。

2.3　比对加密解密行为

采用这样时间空间结合的方式，将用户的行为细化为计算机能够读懂的结构，然后比较加密行为与解密行为是否一致，如果一致，则解密成功，否则解密失败。本文设定时间空间两方面的一致才表示解密成功，即：图形一致；时间一致；落笔、抬笔坐标一致。这 3 个方面缺一不可，当且仅当 3 个方面的要求同时满足才能认为解密成功。在一般加密系统中需要精确匹配，但是同一个人做 2 次相同的事情一定会存在细微的差别，所以不宜采用过高的精度。所以，在本文需要将收集来的时间空间信息模糊化，使得解密过程能够顺利进行。

首先是图形的模糊化。根据数学形态学的腐蚀、膨胀算法，对图像模糊化的数学表达式为：

$$S=X\cup(X\uparrow B)$$

这与图像的细化互补，图像细化的数学表达式为：

$$S=X-X\uparrow B$$

式中↑ 表示的是击中击不中变换，S 是而知图像进行细化后的像素集合，B 表示用来进行细化运算的结构元素，结构元素内的每个元素取值为 0 或 1，他可以组成任何一种形状的图形，在图形中有一个中心点；X 表示原图像经过二值化后的像素集合。此公式的含义是用 B 来细化 X 得到的集合 S，S 是 X 的全部像素点除去击中击不中变换结果后的集合。击中、击不中与包含的关系如图 1 所示。

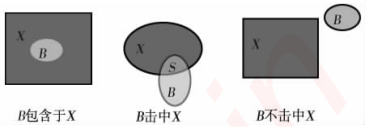

图 1　击中、击不中与包含的关系

在细化一幅图像 X 的过程中应满足两个条件：第一，在细化过程中，X 应该有规律的缩小；第二，在 X 逐步缩小的过程中应到使 X 的连通性保持不变。

图像细化的实现步骤如下：

(1) 获得原图像地址及图像的高与宽；

(2) 开辟内存缓冲区，并初始化为 255；

(3) 如果当前像素为白（背景），则跳过该像素；

(4) 如果当前像素为黑(图像)，则定义一个 5*5 的结构元素，计算 5*5 的结构元素中各个位置上的值；

(5) 依次判断 S 模板点是否满足判定条件，是则删除该点，否则判断下一个像素点，直到所有的像素点处理完一遍；

(6) 循环执行 (5) 直到没有点可以删除为止；

(7) 将结果保存到内存缓冲区。

在图像细化的基础上对图像像素点的灰度值取补，而后调用细化处理函数对取补后的图像进行处理，就得到需要的图像粗化。

加密图形解密图形均用上述步骤粗化，然后做异或运算，统计出异或运算后矩阵中为 1 的元素，再除以粗化后原图形为 1 元素总个数，得到图形容差。公式如下：

$$\text{图形容差}=\frac{\text{异或运算后矩阵中为 1 的元素总个数}}{\text{原图形为 1 元素的总个数}}$$

对于时间的一致，采用如下公式：

$$\text{时间容差}=\frac{|\text{加密过程消逝时间}-\text{解密过程消逝时间}|}{\text{加密过程消逝时间}}$$

对于落笔抬笔的一致，采用如下公式：

$$X\text{ 轴方向容差}=\frac{|\text{加密中对应点 }X\text{ 坐标}-\text{解密中对应点 }X\text{ 坐标}|}{\text{加密中对应点 }X\text{ 坐标}}$$

$$Y\text{ 轴方向容差}=\frac{|\text{加密中对应点 }Y\text{ 坐标}-\text{解密中对应点 }Y\text{ 坐标}|}{\text{加密中对应点 }Y\text{ 坐标}}$$

这里的容差可以根据实际情况设定，开始加密的时候可以有一个学习记忆的过程，实际容差小于设定容差，且上述几个容差同时满足就说明解密成功。

3　系统结构设计与实现

3.1　总体架构及流程

采用 android 系统平台实现这套系统。对于加密模块，当程序启动之后，首先执行初始化，然后绘制人机对话界面，这个界面包含：用户绘图区域和菜单栏。在初始化绘图区域之后开始进入消息循环，捕捉用户在触摸屏上的动作。对用户在触摸屏上的落笔、拖动、抬笔 3 个动作分别连接事件。落笔时需要处理该点坐标，落笔时刻，还需要建立表 1 所示的节点。拖动时相对比较简单，只需要记录所划过点的坐标。抬笔的时候除了记录坐标之外，还需要完成链表的链接工作。用户绘图完成之后点击菜单中的“加密完成”则加密模块完成，。解密时，步骤与加密类似仍然先调用绘图模块，而后在消息循环中不断存储用户行为。在加密解密行为都存储之后按给定的设计方式进行匹配。

3.2　行为加密在 android 上的实现

根据上文的分析，整个系统分为如下几个模块：界面设计模块、绘制图形模块、加密模块、解密模块、匹配模块。加密、解密以及匹配的模块已在上文叙述。界面设计模块以及绘制图形模块参考 google 提供的开发者文档中的例程，以及 activity 的处理机制来实现。需要注意的是 Android 应用程序的基础功能单元就是 Activity—android.app.Activity 类中的一个对象。如 Activity 显示在屏幕上并且设计它的 UI，需要使用 view 和 viewgroup—Android 平台基础的用户界面表达单元。另外在 android 系统平台上开发用户界面，并不像在 VC 等环境中，用所见即所得的方法编辑程序界面，这里是通过 xml 语言控制界面的排列。

4　测试

4.1　测试环境

由于采用 Eclipse3.2 配合 Android SDK 的方式开发，Eclipse 是一种可扩展的开放源代码 IDE。Eclipse 允许在同一 IDE 中集成来自不同供应商的工具，并实现了工具之间的互

（下转第 165 页）

陕北矿业公司综合信息网建设规划

廖晓群[1]，田志英[2]，赵安新[1]

（1. 西安科技大学 网络中心，西安 710054；2. 西安科技大学 通信学院，西安 710054）

摘 要：以信息化带动煤炭工业化，走新型工业化道路，建设新型现代化矿井，是二十一世纪煤炭企业提高矿井安全程度、实现高产高效、增强核心竞争力的必然途径，是煤炭科技发展的方向。陕北矿业公司按照集团公司《信息化总体规划》要求，建设综合信息网平台，实现矿井安全生产和管理各环节全过程的自动化，实现企业管理全面信息化、电子商务和办公自动化，实现生产、管理与控制一体化，提高生产、管理的决策科学化水平，实现全公司数据、信息最大程度的共享。

关键词：煤炭；信息化建设；信息网平台

中图分类号：TP393 文献标识码：B 文章编号：1008-8725（2010）09-0165-03

Integrated Information Network Construction Planning of Mining Company in Northern Shanxi

LIAO Xiao-qun[1], TIAN Zhi-ying[2], ZHAO An-xin[1]

（1. Network Information Center, Xi´an University of Science & Technology, Xi´an 710054, China; 2. College of Communication Engineering, Xi´an University of Science & Technology, Xi´an 710054, China）

Abstract: Using information to promote industrialization of coal, taking a new road to industrialization and building a new modern mine, which is a way for the coal enterprises to improve mine safety, to realize high efficiency and enhance the core competitiveness direction and the coal science and technology development in the twenty-first century. Group mining company in northern Shanxi in accordance with the "information-based master plan" requirement, the building of an integrated information network platform, to realize the mine safety production and management automation of various aspects of the whole process achieves comprehensive enterprise management information, e-commerce and office automation production, management and control integration and improves production management, decision-making and scientific standards, and achieve company-wide data and information to maximize sharing.

Key words: coal; information construction; information network platform

（上接第 160 页）

操作性，从而显著改变了项目工作流程，使开发者可以专注在实际的嵌入式目标上，可使用 GPhone 模拟器作为载体验证本软件的有效性和可行性。

4.2 实例测试

首先启动程序，进入加密部分软件。此时，在用户区域上键入加密行为，如图 2 所示。加密行为键入完成后，点击 MENU 选择“加密完成”，如图 3 所示，至此，加密过程结束。打开解密软件，键入解密行为，如图 4 所示。同样，点击 MENU 选择“加密完成”。最后调用匹配函数判断解密行为与加密行为是否一致，并在屏幕上显示，如图 5 所示。

图 2 键入加密行为　图 3 加密完成　图 4 键入解密行为　图 5 解密完成

5 结束语

通过对行为加密这种新兴加密方式的应用研究，设计了一套适应于移动平台的行为加密应用系统，论述了行为的定义和加解密的判定方法，给出了应用系统的架构与处理流程，并在 Android 平台上用 GPhone 验证了该应用系统，测试结构表明本文给出的行为加密应用系统是有效的和可行的。

参考文献：

[1] 韩青.以商业级 Linux 抓住 Android 带来的商机[J].现代电信科技，2008（1）：24-26.

[2] 黄群.图像比对技术在侦察破案中的应用[J].技术摄影，2003（10）：23-24.

[3] 张津，万振凯.基于数学形态学的图像二值化算法[J].仪器仪表用户，2008（2）：80-81.

[4] 李晓飞.图像腐蚀和膨胀的算法研究[J].影像技术.2005（1）：37-39.

[5] 公磊，周聪.基于 Android 的移动终端应用程序开发与研究[J].计算机与现代化，2008（8）：85-89.

（责任编辑 张欣）

嵌入式资源免费下载

总线协议：

1. 基于 PCIe 驱动程序的数据传输卡 DMA 传输
2. 基于 PCIe 总线协议的设备驱动开发
3. CANopen 协议介绍
4. 基于 PXI 总线 RS422 数据通信卡 WDM 驱动程序设计
5. FPGA 实现 PCIe 总线 DMA 设计
6. PCI Express 协议实现与验证
7. VPX 总线技术及其实现
8. 基于 Xilinx FPGA 的 PCIE 接口实现
9. 基于 PCI 总线的 GPS 授时卡设计
10. 基于 CPCI 标准的 6U 信号处理平台的设计
11. USB30 电路保护
12. USB30 协议分析与框架设计
13. USB 30 中的 CRC 校验原理及实现
14. 基于 CPLD 的 UART 设计
15. IPMI 在 VPX 系统中的应用与设计
16. 基于 CPCI 总线的 PMC 载板设计
17. 基于 VPX 总线的工件台运动控制系统研究与开发

VxWorks：

1. 基于 VxWorks 的多任务程序设计
2. 基于 VxWorks 的数据采集存储装置设计
3. Flash 文件系统分析及其在 VxWorks 中的实现
4. VxWorks 多任务编程中的异常研究
5. VxWorks 应用技巧两例
6. 一种基于 VxWorks 的飞行仿真实时管理系统
7. 在 VxWorks 系统中使用 TrueType 字库
8. 基于 FreeType 的 VxWorks 中文显示方案
9. 基于 Tilcon 的 VxWorks 简单动画开发
10. 基于 Tilcon 的某武器显控系统界面设计
11. 基于 Tilcon 的综合导航信息处理装置界面设计

12. VxWorks 的内存配置和管理
13. 基于 VxWorks 系统的 PCI 配置与应用
14. 基于 MPC8270 的 VxWorks BSP 的移植
15. Bootrom 功能改进经验谈
16. 基于 VxWorks 嵌入式系统的中文平台研究与实现

Linux：

1. Linux 程序设计第三版及源代码
2. NAND FLASH 文件系统的设计与实现
3. 多通道串行通信设备的 Linux 驱动程序实现
4. Zsh 开发指南-数组
5. 常用 GDB 命令中文速览
6. 嵌入式 C 进阶之道
7. Linux 串口编程实例
8. 基于 Yocto Project 的嵌入式应用设计
9. Android 应用的反编译

Windows CE：

1. Windows CE.NET 下 YAFFS 文件系统 NAND Flash 驱动程序设计
2. Windows CE 的 CAN 总线驱动程序设计
3. 基于 Windows CE.NET 的 ADC 驱动程序实现与应用的研究
4. 基于 Windows CE.NET 平台的串行通信实现
5. 基于 Windows CE.NET 下的 GPRS 模块的研究与开发
6. win2k 下 NTFS 分区用 ntldr 加载进 dos 源代码
7. Windows 下的 USB 设备驱动程序开发
8. WinCE 的大容量程控数据传输解决方案设计
9. WinCE6.0 安装开发详解
10. DOS 下仿 Windows 的自带计算器程序 C 源码
11. G726 局域网语音通话程序和源代码
12. WinCE 主板加载第三方驱动程序的方法
13. WinCE 下的注册表编辑程序和源代码
14. WinCE 串口通信源代码
15. WINCE 的 SD 卡程序[可实现读写的源码]
16. 基于 WinCE 的 BootLoader 研究

PowerPC：

1. Freescale MPC8536 开发板原理图
2. 基于 MPC8548E 的固件设计
3. 基于 MPC8548E 的嵌入式数据处理系统设计
4. 基于 PowerPC 嵌入式网络通信平台的实现
5. PowerPC 在车辆显控系统中的应用
6. 基于 PowerPC 的单板计算机的设计
7. 用 PowerPC860 实现 FPGA 配置

ARM：

1. 基于 DiskOnChip 2000 的驱动程序设计及应用
2. 基于 ARM 体系的 PC-104 总线设计
3. 基于 ARM 的嵌入式系统中断处理机制研究
4. 设计 ARM 的中断处理
5. 基于 ARM 的数据采集系统并行总线的驱动设计
6. S3C2410 下的 TFT LCD 驱动源码
7. STM32 SD 卡移植 FATFS 文件系统源码
8. STM32 ADC 多通道源码
9. ARM Linux 在 EP7312 上的移植
10. ARM 经典 300 问
11. 基于 S5PV210 的频谱监测设备嵌入式系统设计与实现

Hardware：

1. DSP 电源的典型设计
2. 高频脉冲电源设计
3. 电源的综合保护设计
4. 任意波形电源的设计
5. 高速 PCB 信号完整性分析及应用
6. DM642 高速图像采集系统的电磁干扰设计
7. 使用 COMExpress Nano 工控板实现 IP 调度设备