Theory and Imitating Input Based on Windows System

基于Windows环境的仿真输入原理与实现

摘要：本文介绍了一种在Windows平台下仿真键盘、鼠标输入的方法，使用此方法可以记录键盘、鼠标的输入，并且模仿记录的键盘、鼠标输入动作，从而模拟人的行为实现程序自动控制。

关键词：仿真 键盘 鼠标 程序控制

陈 炼 刘昌平 （江西 南昌大学计算中心 330029）

1 引言

在实际应用中，有些应用系统要求具有仿真输入的功能，即在没有人为干预的情况下也能够自动进行诸如鼠标点击、键盘输入等动作。本文结合开发机动车辆检测线系统的实践，详细阐述了在Windows环境下实现仿真输入，即在自己的程序中对他人或操作系统的应用程序进行控制，从而模拟人的行为实现自动控制的方法。

目前，各机动车辆检测单位都使用计算机系统实现机动车辆的年度检测，而且需要在不修改原检测系统软件的基础上增设车牌号码识别软件。通过对车辆拍照并识别出牌照号码，将此号码填入到原检测软件指定窗口，最后利用仿真输入模仿原检测软件，使车辆上线接受检测等一系列动作，来实现机动车辆检测的全自动化。

2 基本概念与原理

2.1 Windows 窗口特性及消息机制

Windows系统初启时，创建第一个窗口，即桌面窗口，它是窗口树的根。一个进程创建时，通常由它的主线程建立属于该线程的第一个窗口（有些线程不创建窗口），该窗口成为桌面窗口的子窗口，需要时，建立从属于该窗口的子窗口及其后代，从而构成一棵窗口树。每个窗口用窗口句柄来唯一地标识，此窗口句柄是动态分配的，线程在不同时刻运行，其窗口句柄是变化不定的。根据该句柄，系统通过向窗口发送消息来完成操作与控制。此外，窗口还有诸如窗口类、窗口标题等特性，可以依据窗类名与标题在窗口树中找到特定的窗口。

在Windows平台下，一个线程通常不能直接操作属于另一线程的数据。消息是线程间进行通信的途径之一。每个线程都有自己的消息队列，线程的运行就是不断从消息队列中取出消息并加以处理。Windows是多任务抢占式操作系统，一个线程随时可以停止运行，随后可以调度另一个线程。每隔20ms左右，Windows要查看当前存在的所有线程内核对象，并从可调度的线程内核对象中选择一个，分配CPU资源。Windows维护一个全局消息队列，所有发生的消息都先进入到此队列，然后根据消息附带的参数将此消息发送到指定的线程。

2.2 定义

为了方便后面的叙述，首先给出以下定义：

(1) 定义1：静态子窗口。在进行程序编译时，作为静态资源而存在的窗口称为静态子窗口。静态子窗口包括程序运行时可见的窗口以及物理上存在但被隐藏了的窗口。

(2) 定义2：动态子窗口。在线程运行过程中，动态创建的子窗口称为动态子窗口。例如在程序运行一段代码时，生产新的窗口；点击“打开”、“保存”、“另存为”之类的按钮时弹出的子窗口，都称为该程序主窗口的动态子窗口。这类窗口与其父窗口并列位于桌面窗口之下，但它的父窗口指针指向该线程主窗口。

(3) 定义3：叶窗口 在一棵窗口树中没有后代窗口的窗口称为叶窗口。

3 仿真输入的算法与实现

3.1 数据结构

为了记录每次键盘、鼠标消息的参数，需要建立如下仿真操作数据结构。程序维护一个结构体队列，对于每一次键盘或鼠标操作，均建立一个结构体变量用于存放键盘或鼠标消息的参数，并将此结构体变量置于结构体队列中。在仿真输入时，依次从结构体队列中取出仿真操作参数模仿记录的操作。

```
class CTraceAction
{   unsigned long m_message;
    int m_nXPoint;
    int m_nYPoint;
    CString m_strhwndtitle;
    CString m_strhwndclassname;
    BOOL m_bstaticleaf;
    int m_nindex;
```

```
    CString m_strparenthwndtitle;
    CString m_strparenthwndclassname;

};
```

各成员含义如下：

(1) m_message表示键盘或鼠标消息的代号；

(2) m_nXPoint、m_nYPoint两成员，对于鼠标消息其值为发生鼠标消息的窗口座标位置，对于键盘消息其值为 1；

(3) m_strhwndtitle、m_strhwndclassname、m_strparenthwndtitle、m_strparenthwndclassname 对于鼠标消息分别表示处理该消息的窗口标题、窗口类名、该窗口的父窗口标题及父窗口类名，对于键盘事件为空；

(4) m_bstaticleaf表示处理当前消息的窗口是否为静态子窗口；

(5) 当处理当前消息的窗口是静态子窗口时，m_nindex表示该窗口在叶窗口队列中的次序，对于动态子窗口，其值为-1；

3.2 记录输入动作

在进行输入仿真之前，必须记录要仿真的动作。首先依据给定的窗口标题，在窗口树中找到指定的窗口句柄，然后遍历出该窗口的所有叶窗口，构成叶窗口句柄队列，给定的窗口句柄也加入此叶窗口句柄队列中。要实现输入动作的记录，需借助于Windows的挂钩函数SetWindowsHookEx，它是一个动态链接库文件导出的API函数。动态链接库文件借助此函数将键盘、鼠标回调函数KeyboardProc、MouseProc挂入系统挂钩链中。每当有键盘或鼠标事件时，在将该消息从全局消息队列发送到处理该消息的相应线程之前调用KeyboardProc或MouseProc函数，由此回调函数向主控程序发送自定义消息。主控程序接到该自定义消息时，获取此键盘或鼠标消息的相关参数，并记入到仿真动作数据结构中。

3.3 仿真输入动作

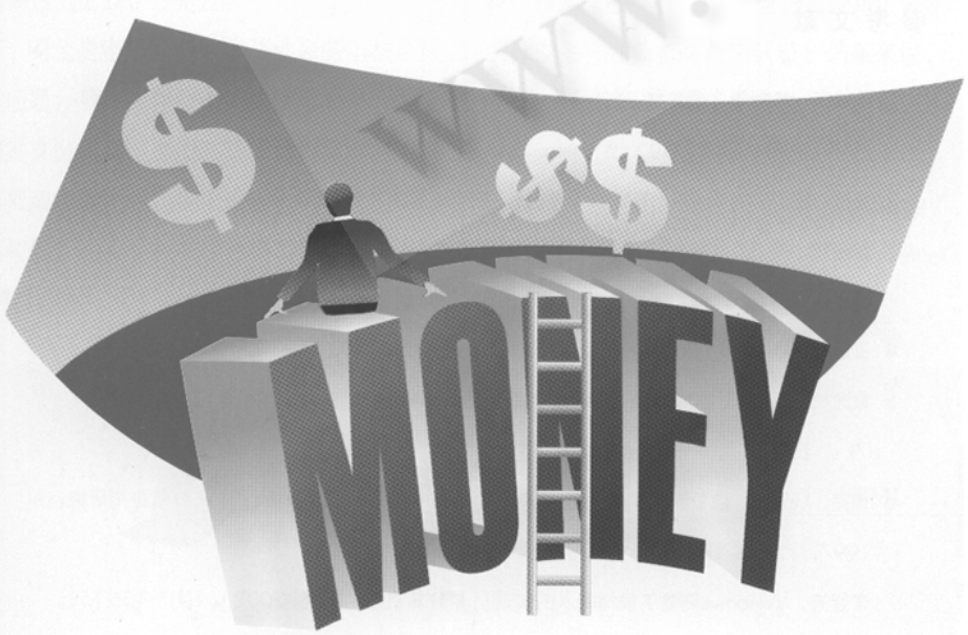
在仿真输入之前，依据此窗口标题在窗口树中找到该主窗口句柄，然后遍历以该窗口为根的窗口树，找出它的叶窗口，产生一个叶窗口句柄队列，该主窗口句柄也记入此叶窗口句柄队列中，叶窗口句柄队列中所指向的窗口都是主窗口的静态子窗口。仿真输入时，从仿真动作数据结构中依次取出消息的参数。如果是发往静态子窗口的消息，则在叶窗口句柄队列中依据该窗口句柄在叶窗口句柄队列中的次序找到此窗口的句柄，对于发往动态子窗口的消息，需要遍历桌面窗口的直接后代以找到该窗口句柄，最后向找到的窗口发送该消息。由于生成动态窗口需要的时间往往多于程序仿真一个事件的时间，仿真程序在模拟完一个事件之后，需要睡眠一段时间以等待上一事件完全结束。

遍历窗口树，构造叶窗口句柄队列算法如下：

```
找到指定窗口标题的窗口句柄wndTarget;
wndTarget入栈wndStack;
while 栈wndStack非空
    {
wndStack出栈wndTemp;
    遍历以wndTemp为根的子窗口
    if wndTemp有子窗口
            wndTemp所有子窗口入栈wndStack
    else
        wndTemp入栈wndLeaf
    }
wndTarget入栈wndLeaf
```

模拟键盘、鼠标输入事件算法如下：

```
置窗口wndTarget为前台;
for i =1 to 事件结构体队列中事件的个数
{   睡眠一段时间
    if 事件i 是鼠标事件
        {
        if m_bstaticleaf=1
            取出事件结构体i 的数据，发送消息
        else
            遍历桌面窗口的直接后代，找到接受消息的窗口句柄wndDyn;
            遍历wndDyn的叶窗口，构造wndDyn的叶窗口句柄队列wndDynLeaf
            在wndDynLeaf中以窗口标题及类名找处理该事件的窗口wndEvent
            向窗口wndEvent发送消息;
    }
```

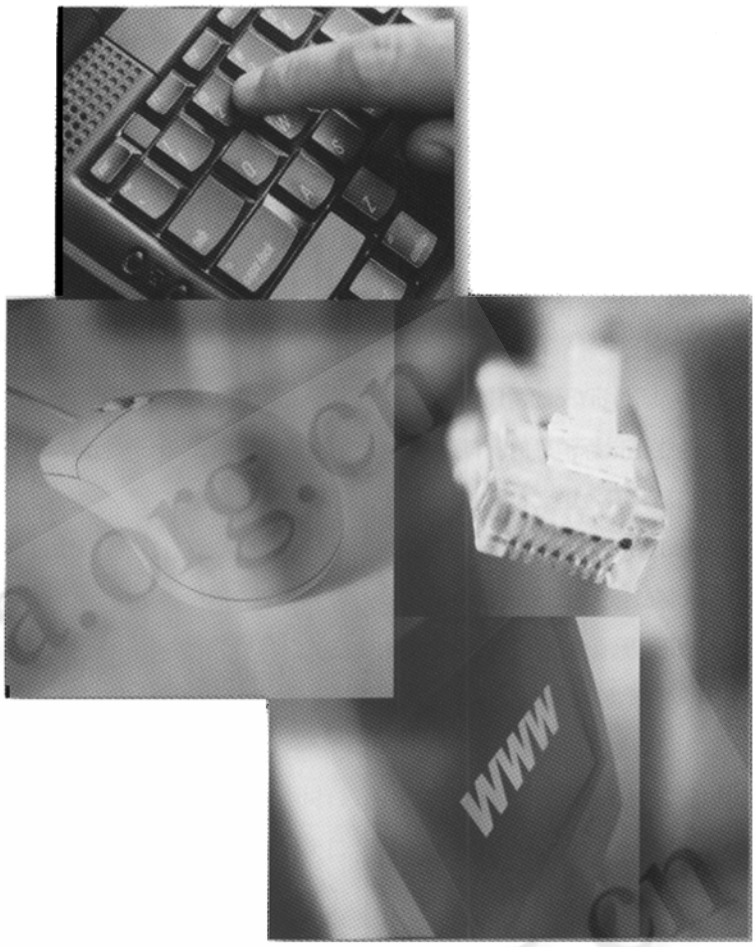


```
        else if事件i 是键盘事件
            使用keybd_even 模拟键盘事件
    }
```

4 结束语

通过研究国内外模拟输入的技术资料及软件产品，发现绝大多数的模拟技术都是通过记录键盘、鼠标事件宏来达到模拟输入的目的，目标窗口的位置一旦改变，整个模拟过程就发生混乱，只看到鼠标指针在屏幕上移动，却达不到预期的效果。本文的仿真输入过程利用Windows消息机制，通过发送记录下来的消息来达到仿真目的，即使是在窗口状态改变的情况下，仍能达到预期的效果。经实践，将此模拟过程放在机动车辆年度检测线控制系统中，能完全仿真键盘点击、鼠标单击、双击，达到模拟人工操作的目的。

由于在记录鼠标移动、拖动事件时需要记录的事件数量非常巨大，建立的事件结构体也很多，模拟这些事件所需的时间开销大，所以此仿真输入没有考虑模仿这些事件的操作。



参考文献

1 陈毅东、李绍滋、李堂秋，利用Windows消息实现应用程序控制[J]，计算机应用研究，2001，4(4)：98-101。

2 金贵，关于Windows98的窗口结构[J]，昭乌达蒙族师专学报，2000，6(3)：36-41。

3 张聪娥、曹进克，Win32系统窗口消息传送技术分析[J]，信息工程大学学报，2002，3(1)：54-57。

4 王建华，Windows核心编程[M]，机械工业出版社，2000.142-143。

5 戴逸民、郭东风、胡熠，利用钩子函数截获Windows消息[J]，微型机与应用，1999，7(7)：15-17。

6 杨亮、阮晓星、魏晋鹏，Windows消息驱动机制中的核心技术分析[J]，计算机应用研究，1997，12(5)：12-14。

7 李智芳，Windows环境下模拟输入的实现[J]，计算机应用研究，2002.，1(1)：156-158。