[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710196737.5

[43] 公开日 2009 年 5 月 27 日

[11] 公开号 CN 101441689A

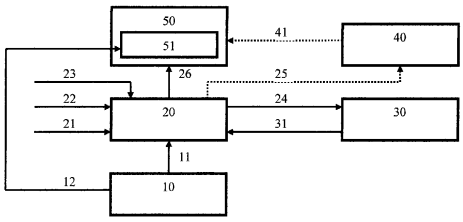
[22] 申请日 2007.11.23
[21] 申请号 200710196737.5
[71] 申请人 杨筑平
地址 523106 广东省东莞市莞城区第二教师村 2 栋 301
[72] 发明人 杨筑平 周跃平 杨 霄
权利要求书 1 页 说明书 5 页 附图 1 页

[54] 发明名称

登录保护方法

[57] 摘要

登录保护方法，涉及计算机软件、网络通信和信息安全技术领域。 于目标登录界面之外，用一代理程序收集用户登录信息，至少对其中密码项施行加密变换，待用户实际操作指向目标登录界面上待发送去向的子窗口位置，再通过窗口消息跨越线程发送到目标登录界面；自我主动为窗口归属线程动态抢占安装防御性勾子(Hook)程序，竞争使之处于勾子链头而将被系统优先调用执行，防御性勾子程序终极径直返回而屏蔽后续勾子，阻止恶意截获窗口过程相关消息。 本发明可实现通用软件产品和网上服务系统，代理程序独立于目标应用程序并发运行，普适于电子信箱、网上银行、商务、政务、通信、游戏，以及各种凡需用户登录的信息系统，能有效保护用户帐户免被盗用。



1、一种登录保护方法，是由登录程序为自己的登录窗口的归属线程主动安装防御性勾子程序，用来阻止其他线程安装的同类勾子程序截获窗口过程相关消息，其特征在于：所述主动安装是动态抢占式安装，倾向于竞争成为最新安装的勾子，使所述防御性勾子程序处于同类勾子链上头节点而将被系统优先调用执行，所述防御性勾子程序的终极处理则是直接返回而不调用勾子链上后续节点的其他勾子程序，从而达到屏蔽其他勾子程序的功效目的。

2、根据权利要求 1 所述的方法，其特征在于，所述动态抢占式安装，通过窗口及其控件事件驱动或定时器事件驱动，即时响应实施安装，而竞争的策略则是脉动式地反复地卸载再安装。

3、一种登录保护方法，是于目标登录界面之外，用另一个代理程序呈现可与之参照的替代输入界面，收集用户的登录信息，然后通过窗口消息传递方式跨越线程发送到目标登录界面，其特征在于：在用户确认登录信息之后，所述代理程序还等待用户实际操作指向目标登录界面上待发送去向的具体子窗口位置，而且所述代理程序在登录信息被发送之前或者在登录信息被送达目标登录界面之前，至少对其中的密码项施行加密变换。

4、根据权利要求 3 所述的方法，其特征在于，所述代理程序还自含独立认证体系，包括采集、登记、验证终端本机特征数据的步骤，和/或采集、登记、验证终端外部输入特征数据的步骤。

5、根据权利要求 4 所述的方法，其特征在于，所述认证体系的登记和验证步骤，经由联网布置的认证服务器来实施。

6、根据权利要求 3 所述的方法，其特征在于，所述由用户实际操作指向的具体子窗口位置为登录信息的初始项位置，而登录信息的后续项位置则由所述代理程序依序操控指向。

7、根据权利要求 6 所述的方法，其特征在于，所述后续项位置被操控定位于目标登录界面上的一个用于确认登录的按钮或其他类型控件，所述代理程序随后通过模拟键盘回车按键或鼠标点击动作，而触发在目标登录界面上的登录行为。

8、根据权利要求 3 所述的方法，其特征在于，所述加密变换所采用的算法或密钥，与终端的本机特征数据和/或外部输入特征数据相关联。

9、根据权利要求 3 所述的方法，其特征在于，所述加密变换所采用的算法或密钥，经由联网布置的认证服务器来实现和提供。

10、根据权利要求 3 所述的方法，其特征在于，所述用户实际操作指向，还导致所述代理程序为所指向子窗口的归属线程安装防御性勾子程序，以此屏蔽此前由其他线程在先安装的同类勾子程序。

登录保护方法

技术领域

本发明涉及计算机软件、网络通信和信息安全技术领域。

背景技术

登录，是用户进入和使用应用系统的必由之路。在登录界面上，用户输入登录信息（主要是帐户信息，包括用户名/帐号、密码，还可能有验证码之类的辅助信息），确认之后接受系统核验。在网络环境，尤其是在互联网上，形形色色的间谍程序（指盗窃用户信息的程序，如木马程序等）横行肆虐，却又十分隐密难以发现，经常在用户不知不觉中窃取帐户信息，侵犯用户隐私和财产。这已经成为网络社会的一大公害，极大地危及电子信箱、网上银行、电子商务、电子政务、即时通信、网络游戏等各种应用的正常秩序。

间谍程序窃取用户登录的帐户信息，主要有三种手段：一是窃听键盘，记录按键和鼠标操作信息；二是偷窥屏幕，截取窗口界面图象；三是拦截消息，获取窗口输入信息。现有技术的各种对抗措施和解决办法也已经不断涌现。“基于图形键盘的计算机信息安全输入方法”（中国发明专利申请号 200410050950.1）和“内容输入方法及其系统”（中国发明专利申请号 200710109498.5）的办法是，呈现图形键盘界面，将鼠标输入点击位置转换为字符输入。这样的方法避开了窃听键盘记录按键，却瞒不过偷窥屏幕。间谍程序只要将前两种手段结合使用，既记录鼠标点击位置，又截取键盘图形，就能有效破解再现输入的字符信息。“动态识别方法”（中国发明专利申请号 200510025109.1）的办法是，由用户预设变化规则，通过随机交互问答进行认证，给偷窥制造困难。这种方法较繁琐而且仍然不能有效躲避间谍程序。“用于防止非法程序窃取用户信息的方法及装置”（中国发明专利申请号 200610105978.X）的办法是，根据对进程行为的判断以决定是否拦截系统调用，为求有效需要触动操作系统内核。这种方法比较复杂，要做到准确判断实际会很困难，而且若触动系统内核也有稳定性之虞，何况还有操作系统版本升级的变数。其以为拦截发送 WM_GETTEXT 消息对阻止窃取文本信息是充分的，其实是不够的；而且，还不能解决窃听键盘和偷窥屏幕的隐忧。综上所述，现有的技术方法，对于防止登录过程中用户的帐户信息被盗用，都还有一定的局限性。

发明内容

本发明提出的登录保护方法，其目的和用途是保护用户的帐户信息在登录过程中免被他人蓄意盗用。

本发明首先从勾子防护这方面入手，其基本思路，是自我主动管制登录窗口的归属线程的勾子链，防备勾子被不良线程恶意利用，切断间谍程序所安装勾子的运行途径。

当今主流的基于图形窗口界面的操作系统（如微软公司的 Windows 系列操作系统），都是通过消息驱动的。多个任务或应用程序能够在宏观上并发运行，每一个任务作为一个进程管理调度，而每一个进程又由一个主线程和若干个（也可以没有）子线程组成。线程是运行调度的基本单元，有自己的输入队列和消息队列。所有窗口都是由对应的线程创建的，本发明将创建某个窗口的线程称为该窗口的归属线程。所有窗口都从属于各自既定的窗口类，也就有相应的窗口过程。输入队列中的输入（如键盘键的按下、弹起，鼠标的移动、点击等动作），都将被转化为消息传递到窗口过程，然后如可见的话再呈现在窗口上。操作系统的一个关键机制，是允许为线程安装勾子（Hook），使得勾子程序代码能够插入线程的执行过程而有机会运行。勾子被分为多种类型，按链式组织管理，各种类型的勾子的宿主和数量不限。操作系统在以窗口消息调用窗口过程之前或之后（依勾子的类型而定），还将窗口消息传给勾子程序并调用执行，于是，勾子程序便能够轻易地获取窗口消息，从而也获得窗口输入。操作系统的勾子机制，既对应用程序的跟踪、调试和监控提供了便利，同时也给了居心叵测的程序以可乘之机。事实上，一些间谍程序所采取的高明手法，正是利用了这一勾子机制作为后门，将遂行盗窃行为的代码作为勾子程序隐蔽地插入窗口（例如用户登录界面窗口）的归属线程，蓄意拦截获取用户信息（例如登录信息）。本发明在这方面的对策，是主动安装防御性勾子，来克制恶意的勾子。操作系统的勾子管理机制，其中有两个关键环节：一是总调用勾子链上头节点的勾子程序；二是依赖于勾子程序的显式调用而将执行转向后续节点的勾子程序。本发明充分利用这两点来构建勾子防护机制。首先，将勾子链上头节点视为至高点，实施动态抢占式的安装，力图通

过竞争使防御性勾子成为最新安装的勾子，即处于同类勾子链上的头节点位置，从而使防御性勾子程序赢得将被操作系统优先调用执行的机会。其次，对防御性勾子程序作出刻意安排，让其直接返回而不再调用勾子链上后续节点的其他勾子程序。防御性勾子程序通常只需是空的回调函数，其除了返回之外什么也无须做；尽管还可以安排承担其他某些附加功能（如字符加密、消息反馈等），但其终极处理则是直接返回，使得勾子链上后续节点的其他勾子程序失去激活执行的机会，从而达到屏蔽其他勾子程序（包括间谍程序安装的勾子程序）的功效和目的。至于屏蔽其他勾子程序是否会有副作用，本发明方法从登录程序功能的单纯性和保护必要性的角度推断，假如登录界面窗口的归属线程被安装了其他勾子，那么这些勾子不是多余的就是不善的，屏蔽它们也不至于造成窗口功能（即用户登录）的缺失和异常。防御性勾子程序虽不能避免间谍程序安装勾子，但凭借抢占优先和直接返回的保障措施，巧妙而又可靠地剥夺了间谍程序勾子的激活执行机会。为了实现动态抢占式的安装，时机的把握，可以安排由窗口事件（如创建、活跃、尺寸改变等）及其控件（即子窗口）的事件（如焦点变化、文本改变、点击等）消息驱动而响应安装。窗口及其控件的事件消息的生成具有随机性，作为对消息的响应而实施安装便是动态的。比如，对于用户登录界面窗口，每当敏感信息项（如用户名、密码）的输入编辑框控件（是子窗口）获得焦点，或确认登录的按钮（也是子窗口）被点击，而产生相应的窗口事件消息时，则予以响应即时安装一次防御性勾子。既然是动态抢占式的安装，就不是一次性安装成功了事，而是倾向于保持竞争态势，脉动式地、反复地，每当预定事件发生时，即实施一次安装。还可以设置定时器，周期性地重复安装防御性勾子。每一次安装都要先卸载旧勾子（初次安装除外）再安装新勾子，而反复安装所用的却是同样的勾子程序（可以是本线程代码域内的局部代码，或是从动态库 DLL 文件加载的全局代码），不会导致勾子数量的累积递增。如此脉动式地、反复地卸载再安装，是与间谍程序竞争勾子优先权的有效策略，使得让防御性勾子抢占并保持在勾子链上头节点成为可能。登录程序为自己的窗口归属线程主动安装防御性勾子，尤其是注重动态抢占式安装，就能够达到自我保护的良好功效。

本发明另一方面的思路，是通过代理收集和加密转换，隐蔽地传递登录信息。

用户登录的基本方式，是直接通过键盘输入登录信息。间谍程序只需周期性地察看输入队列，或监测键盘状态，就能记录窃取用户输入的登录信息。本发明设计采用代理程序，呈现一个替代的输入界面供用户输入登录信息。用户原本要登录的目标应用系统的登录界面，本发明称之为目标登录界面。代理程序的输入界面与目标登录界面是可参照的，前者的信息项输入控件与后者的信息项输入控件至少有部分对应，比如用户名项相对，密码项相对，控件的类型相同或相似；但也无须要求两者的信息项输入控件完全对应，特殊的情形是代理程序的输入界面只有一个信息项（例如密码）输入控件。代理程序在收集了登录信息，并经过用户确认之后，再通过窗口消息传递方式跨越线程而发送到目标登录界面。在操作系统中，可以从一个窗口将消息传送到另一个窗口，具体有两种传送方式：第一种是发送（Send），将消息视为非队列化消息，旁路消息队列而直接调用窗口过程，并等待其执行完毕才返回；第二种是递送（Post），只简单地将消息送入消息队列便立即返回，而任由线程的消息循环去完成后续的提取、分析消息和调用窗口过程。本发明所说的发送，广义地包括这两种传送方式。由于在多任务运行环境，代理程序与目标应用系统（或目标登录程序），甚至还与其他程序并发运行，所以代理程序难以自行确定目标登录界面窗口，更难以确定其中的具体子窗口位置。于是约定，由用户于确认登录信息之后，再实际操作指向目标登录界面上待发送去向的具体子窗口的位置。用户的实际操作指向动作，可以有多种方式。简单的如移动鼠标到位后点击；繁琐的则用功能组合键切换窗口和 Tab 键游历定位后回车确认。用输入笔点选、屏幕手指触摸，可视同鼠标点击。代理程序判断用户已经完成实际操作指向，有两种方式：一是对用户操作动作的检测感知，如鼠标点击、键盘回车键按下；二是定时约定，当预定时间段（如 2 秒钟）逝去，则断定用户已经在此期间完成了实际操作指向。在用户于目标登录界面上实际操作指向之后，操作系统使得目标登录界面窗口成为当前活跃窗口，而光标（焦点）所在的具体子窗口位置也已经可辨。代理程序能够对此作出准确的判定并获取窗口指针（Handle），该所指向的子窗口位置正是目标登录界面上待发送去向的具体子窗口位置。特别地，代理程序在将登录信息发送出去之前，或者至迟在登录信息被送达目标登录界面之前，对登录信息（其中至少包括对密码项）施行了加密变换。于是，从代理程序界面输入的登录信息成为名义登录信息，而经过加密变换后的登录信息才是用于目标登录界面的实际登录信息。间谍程序即使通过监测键盘等办法窃取

了名义登录信息，却不是实际登录信息，不能直接在目标登录界面有效登录。如此，就达到了让用户隐蔽登录的保护效果。

然而，由于代理程序是公开发布的，盗窃者也有机会使用同样的代理程序以窃取的名义登录信息进行登录，就会导致隐蔽登录保护失效。为解决这个问题，代理程序自有独立的一整套认证体系。代理程序的所有用户都有自己的认证帐户，即使用帐户（包括帐号、密码），这是认证管理的基础。代理程序在用户注册或变更时，还自动采集和登记用户终端的本机特征数据，可以选择地，还采集和登记用户终端的输入特征数据。所述本机特征数据，是指终端的硬件配置参数（如CPU类型和序列号、网络适配器物理地址、内存容量、硬盘容量等）、软件环境参数（如操作系统、数据库系统的版本号、序列号、安装日期等）、和存储参数（如配置文件关键数据项、关键识别文件、特定文件在硬盘上的储存位置等），诸如此类足以区别不同终端的设备特征的数据集合。所述输入特征数据，是指由用户从终端外部连接的装置输入的数据，如IC卡、磁卡、USB接口存储器上保存的编码数据，以及指纹、掌纹、虹膜等生物特征数据，等等。代理程序在用户使用于登录时，除了验证认证帐户之外，还将验证终端的本机特征数据和/或输入特征数据。假如盗窃者窃取了名义登录信息，也使用同样的代理程序进行登录，但其却难以异地（在不同终端上）复制合法注册用户终端的本机特征数据，代理程序验证终端本机特征数据的步骤将注定其非法登录失败；即使盗窃者有机会在同一台终端上假冒登录，又因其不能提交有效的输入特征数据，代理程序验证终端输入特征数据的步骤也将注定其非法登录失败。上述认证体系的一种简化实现，是忽略所有登记和验证步骤，而只读取终端输入特征，用做对登录信息施行加密变换的密钥。但出于使用便利、服务效率和安全性乃至营运上的考虑，可以联网布置至少一台认证服务器，而将上述认证体系的登记和验证步骤，经由该认证服务器来实施。

当代理程序收集的登录信息包含有多项信息（如有用户名、密码、验证码），用户确认之后要能够一次性发送到目标登录界面的对应信息项上，前提是这些信息项在代理程序输入界面上的顺序与在目标登录界面上的顺序一致。代理程序实际上是按顺序逐个信息项发送的：发送一个信息项之后，控制移动光标（即焦点）到下一个位置，再发送下一个信息项；如此循环，直至全部信息项发送完毕。因此，由用户实际操作指向目标登录界面的具体子窗口位置即为登录信息的初始项位置，而登录信息的后续项位置则由代理程序依序操控指向。代理程序依序发送完登录信息之后，还可以操控将后续项位置定位于目标登录界面上的一个用于确认登录的按钮或其他类型控件上，随后通过模拟键盘回车按键或鼠标点击动作，而触发在目标登录界面上的登录行为。

为了实现从名义登录信息到实际登录信息的加密变换，可以选用各种加密算法或密钥。而为了增强加密的效果，可以将加密变换的算法确定和密钥选择，与终端的本机特征数据和/或外部输入特征数据相关联。在联网条件下，还可以借助网上布置的认证服务器，来为加密变换实现所用的算法或提供所需的密钥。

在代理程序即将发送登录信息到目标登录界面窗口时，间谍程序可能已经安装了勾子程序准备拦截获取。作为这种情形的防备措施，代理程序在用户实际操作指向之后，即为所指向子窗口的归属线程安装防御性勾子程序，以此来屏蔽此前由其他线程（包括间谍程序的线程）在先安装的同类勾子程序。然后，代理程序才安全地发送登录信息。代理程序也可以视为一种特殊的登录程序，完全可以为自己主动安装防御性勾子程序，自我保护不被间谍程序的恶意勾子程序所骚扰。

本发明的登录保护方法具有通用性，可以实现为软件产品和网上服务系统。所述代理程序独立于目标应用程序而并发运行，能够普遍适用于电子信箱、网上银行、电子商务、电子政务、即时通信、网络游戏，以及各种管理信息系统凡是需要用户登录的场合。

附图说明

图 1 是本发明的登录保护方法的示意图。终端用户（10）使用代理程序（20）输入登录信息（11）；代理程序（20）在收集的登录信息（11）被确认之后，采集本机特征数据（21），和/或采集输入特征数据（22），然后向认证服务器（30）发出认证请求（24）；认证服务器（30）对接收到的认证请求（24），比对此前登记的注册信息，验证终端用户的帐户信息，以及验证终端的本机特征数据和/或输入特征数据，然后发回认证结果（31），其中包含有关加密算法或密钥的信息，或经过加密转换的登录信息项；代理程

序（20）收到认证结果（31）之后，若确定认证有效，则加密转换已收集的登录信息（11），或者就取用回传的已经加密转换的登录信息，等待指向反馈（23）的到来；终端用户（10）在确认登录信息（11）之后，再实际操作指向（12）目标登录界面窗口（50）上的初始项子窗口（51），系统由此将发出指向反馈（23）；代理程序（20）在获得指向反馈（23）之后，立即执行安装勾子（25）行动（虚线示意），使防御性勾子程序（40）能够抢占勾子链头（41）位置（虚线示意），紧接着，以加密转换后的登录信息，作为登录消息（26）发送到目标登录界面窗口（50）。

图 2 是本发明的登录保护方法中，代理程序在一次登录处理过程中的流程图。准备（1）就绪之后，收集登录信息（2），提取特征数据（3）；执行认证（4）过程，判断（5）认证结果，若无效（N）则转向结束（10），若有效（Y）则加密登录信息（6）；判断用户指向（7），若未指向（N）则继续循环等候判断，若已指向（Y）则安装防御性勾子（8）；最后是发送登录消息（9），并结束（10）。

具体实施方式

设定目标运行环境为微软公司的 Windows 操作系统，使用 Visual Studio.Net 集成开发平台。

一、勾子防护的实施方式。

开发一个 Visual C++类型的 MFC 动态链接库（DLL）项目，只建立一个空的回调函数

```
LRESULT CALLBACK RecoveryCallWndProc(int nCode, WPARAM wParam, LPARAM lParam) {
    //return CallNextHookEx();
    return NULL;
}
```

作为防御性勾子程序，其中的代码只是执行返回 0 值，而不执行返回 API 函数调用 CallNextHookEx()，故意地剥夺了后续勾子的运行机会。该 DLL 项目编译生成 recovery.dll 文件。针对所需保护的登录程序，取得其窗口指针 hWnd，再调用 API 函数取得并保存其归属线程的标识

```
dwWinThreadID = GetWindowThreadProcessId(hWnd, NULL);
```

周期性地监测其窗口，每当其成为当前活跃窗口时，则执行类似下列代码段以安装防御性勾子程序

```
HOOKPROC hkprcRecovery;
static HINSTANCE hinstDLL;
static HHOOK hhookRecovery = null;  // 仅初始化一次

hinstDLL = LoadLibrary((LPCTSTR) "recovery.dll");
hkprcRecovery = (HOOKPROC)GetProcAddress(hinstDLL, "RecoveryCallWndProc");
if(hhookRecovery!=null)
    UnhookWindowsHookEx(hhookRecovery);
hhookRecovery = SetWindowsHookEx(idHook, hkprcRecovery, hinstDLL, dwWinThreadID);
```

其中，idHook 是勾子类型（如 WH_CALLWNDPROC、WH_CALLWNDPROCRET、WH_KEYBOARD，等）。为求保险，依次对所有勾子类型（已知现有 15 种），分别如上执行安装防御性勾子程序。再设定一个定时器，在目标应用程序活跃运行期间，每隔 2 秒钟便重复为其如此安装防御性勾子程序，即实现动态抢占式安装。

二、登录保护方法的实施方式。

创建一个解决方案，包括 5 个 Visual C++类型的 Windows 项目：1 个 MFC 动态链接库（DLL）项目，与前面勾子防护的实施方式所述类似，作为安装防御性勾子程序；2 个 MFC 应用程序项目，分别作为代理程序（客户端）和认证程序（服务端）；2 个安装部署项目，分别为代理程序（包括 DLL 项目主输出）和认证程序编译生成安装包。

代理程序，运行于用户终端。设计程序界面，包括三个属性页：[登录]、[认证]、[设置]。[登录]默

认为第一属性页，其中布置3个文本编辑框控件，分别命名为用户名、密码、验证码，每项命名前均配置一个复选框以便选择组合，另外还布置一个[确认]按钮。用户在选择并输入登录信息之后，点击[确认]按钮，代理程序就作出响应，收集登录信息，提取网卡的物理地址编号作为本机特征数据，连同密码项和认证帐户信息，打包为认证请求包，建立TCP/IP连接发送至认证服务器，并在接收到认证结果后拆除TCP/IP连接。认证结果若有效，则其中包含发回的已经加密的密码项，再循环执行API函数检测键盘状态

SHORT state = GetAsyncKeyState(VK_LBUTTON);

直至等到state值对应的鼠标左键状态位置位，即用户已经实际操作点击鼠标指向了目标登录界面窗口内具体子窗口的位置，则获取其窗口指针hWnd，然后按前述勾子防护的实施方式，安装防御性勾子程序。紧接着，对每一个登录信息项，即用户名、密码、验证码（用户如果复选了的话），依序分别调用API函数进行发送

SendMessage(hWnd, WM_SETTEXT, (WPARAM)0, (LPARAM)strItem);

其中，hWnd是目标登录界面窗口内具体信息项子窗口的指针，strItem是要发送的登录信息项字符串的指针。每发送了一条信息项，就调用API函数模拟一次Tab键

keybd_event(VK_TAB, 0, 0, 0);

即可操控光标转移到下一个信息项子窗口。如此重复，直至全部登录信息项发送完毕，目标登录界面窗口上的焦点可能已经移位于确认登录的按钮上，此时再调用API函数模拟回车键

keybd_event(VK_RETURN, 0, 0, 0);

就会触发在目标登录界面上的登录行为。

[认证]为第二属性页，其中布置4个文本编辑框控件，分别命名为认证编号、认证密码、确认密码、输入密钥（输入特征数据），另外还布置一个[确认]按钮。用于管理用户的认证帐户。

[设置]为第三属性页，布置若干控件，用于配置相关参数，如端口、通信方式、速率、数据格式等。

认证程序，运行于服务器端。其主要功能，是在网上及时接受用户终端请求的TCP/IP连接，完成对认证帐户和特征数据的登记和验证，并回传验证结果。特别地，还承担对用户登录密码项进行加密变换，加密算法采用MD5散列算法并按密码长度截取。

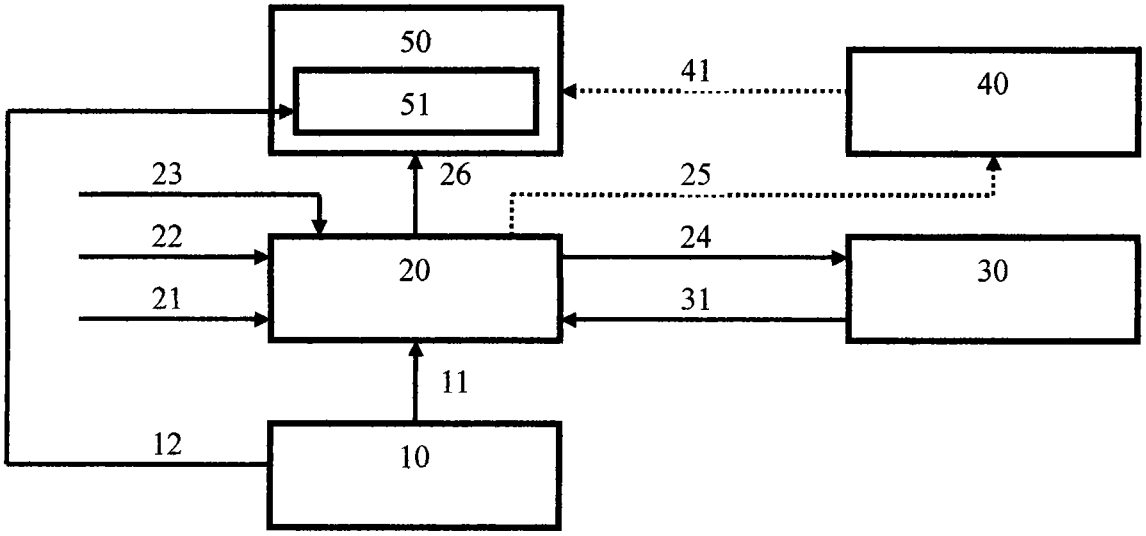


图 1

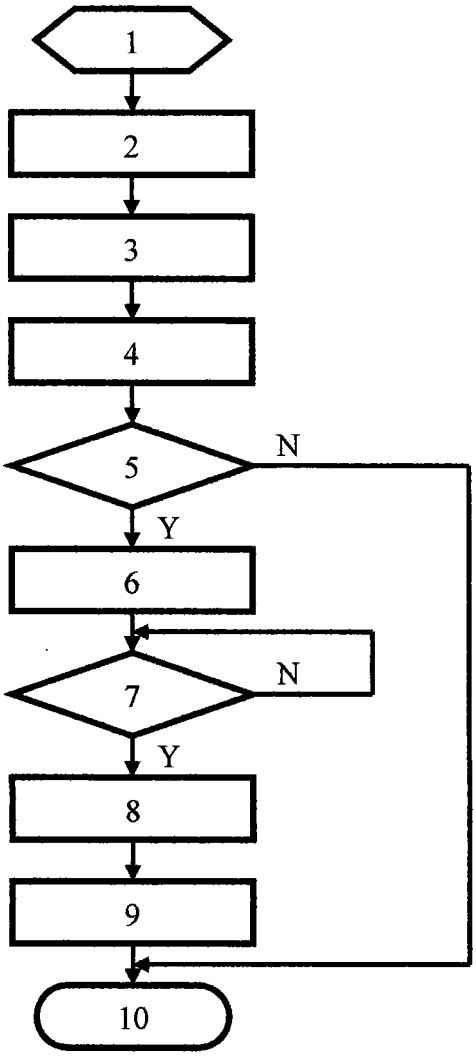


图 2