



(12) 发明专利申请

(10) 申请公布号 CN 104299146 A

(43) 申请公布日 2015. 01. 21

(21) 申请号 201410642932. 6

(22) 申请日 2014. 11. 14

(66) 本国优先权数据

201410432280. 3 2014. 08. 29 CN

(71) 申请人 黄世纬

地址 610000 四川省成都市电子科技大学沙河校区微固学院 2014210301 班

(72) 发明人 黄世纬

(51) Int. Cl.

G06Q 30/00 (2012. 01)

G06F 17/30 (2006. 01)

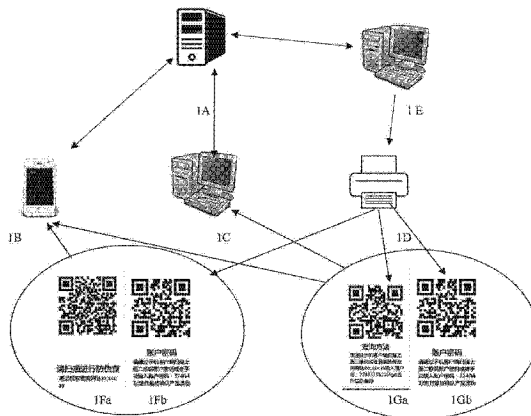
权利要求书3页 说明书5页 附图3页

(54) 发明名称

一种产品防伪查询系统

(57) 摘要

一种产品防伪查询系统,包括数据库服务器、移动客户端或者PC客户端、厂家后台或者数据库服务器操作后台,其中数据库服务器用于注册产品注册账户,移动客户端或者PC客户端用于查询产品注册账户信息,厂家后台或者数据库服务器操作后台用于在产品注册账户中登记产品信息。本发明在保证在售产品不被破坏原防伪验证密码的情况下提供多次初次防伪查询,并且防止因防伪密码被恶意暴力破解导致在售商品在出售防伪验证时显示为伪劣产品。



1. 一种产品的防伪系统,包括数据库服务器、移动客户端或者 PC 客户端、厂家后台或者数据库服务器操作后台;其中,

数据库服务器用于提供厂家通过厂家后台或数据库服务器操作后台在数据库服务器中注册产品注册账户以及用于存储厂家通过厂家后台数据库服务器操作后台在数据库服务器注册产品注册账户的用户名和密码以及用于存储厂家通过厂家后台数据库服务器操作后台在所述产品注册账户里登记的产品信息或者厂家信息,以及接受移动客户端或者 PC 客户端发送的所述产品注册账户的用户名和密码并进行认证并且在认证正确的情况下,除了反馈给移动客户端或者 PC 客户端厂家在所述产品注册账户里登记的商品信息或者厂家信息外,如果这是第一次认证正确,则反馈给移动客户端或者 PC 客户端所查询商品为全新正品信息或者所查询次数为第一次,如果这是第二次或以上次数认证正确,则反馈给移动客户端或者 PC 客户端所述产品注册账户已被激活的信息,所述激活的信息即让消费者清楚所述产品注册账户在其之前已被登录,或者提示消费者所查询产品涉嫌假冒伪劣的信息,以及接受移动客户端或者 PC 客户端发送的所述产品注册账户用户名并进行认证或者接受移动客户端发送的查询产品注册账户的网址认证,并且在认证正确的情况下,反馈给移动客户端厂家已在所述产品注册账户里登记的商品信息或者厂家信息或者所述产品注册账户是否已被激活信息或者提醒客户输入账户密码进行下一步认证;

移动客户端接用于接受客户输入所述产品注册账户用户名并将所述用户名发送至数据库服务器并接受数据库服务器反馈的信息并显示给客户以及用于接受客户输入所述产品注册账户用户名和密码并将所述用户名和密码发送至数据库服务器并接受数据库服务器反馈的信息并显示给客户,或者用于解析表达所述产品注册账户网址的二维码,并将通过所述网址访问数据库服务器并接受数据库服务器反馈的信息,所述产品注册账户网址即通过该网址即可访问所述产品注册账户查看厂家已在所述产品注册账户登记的商品信息或者所述产品注册账户是否已被激活信息,或者用于解析表达所述产品注册账户用户名和密码的二维码或条形码,并将所述产品注册账户用户名和密码发送至数据库服务器并接受数据库服务器反馈的信息并显示给客户,或者用于解析表达所述产品注册账户用户名的二维码或条形码,并将所述产品注册账户用户名发送至数据库服务器并接受数据库服务器反馈的信息并显示给客户;

PC 客户端用于接受客户输入所述产品注册账户用户名并将所述用户名发送至数据库服务器并接受数据库服务器反馈的信息并显示给客户以及用于接受客户输入所述产品注册账户用户名和密码并将所述用户名和密码发送至数据库服务器并接受数据库服务器反馈的信息并显示给客户;

厂家后台或者数据库服务器操作后台用于向数据库服务器注册所述产品注册账户并在所述产品注册账户登记厂家信息或者产品信息并将所述产品注册账户的用户名和密码导出来,所述产品注册账户的用户名和密码包括人为生成或者随机生成。

2. 根据权利要求 1 所述的系统,其特征在于:所述系统还包括打印设备,所述打印设备将接受厂家后台或者数据库服务器操作后台输出的所述产品注册账户用户名和密码并将其打印出来,如果将所述产品注册账户用户名和密码用条形码或二维码表示,则所述系统增加条形码或二维码编码设备或者在所述厂家后台或者数据库服务器操作后台安装条形码或二维码编码软件,所述编码设备或者条形码或二维码编码软件将表达出所述产品注册

账户用户名和密码的条形码或者二维码输入打印设备,并将其打印出来,或者如果将查询所述产品注册账户的网址采用二维码表示时,将查询所述产品注册账户的网址输入二维码编码设备或者条形码或二维码编码软件,并将表达成的二维码输入打印设备并将其打印出来,所述查询产品注册账户网址即为通过该网址即可访问所述产品注册账户查看厂家已在所述产品注册账户登记的商品信息以及所述产品注册账户是否已被激活信息或者客户已登记的个人信息。

3. 根据权利要求 1 所述的系统,其特征在于:数据库服务器还用于,在厂家通过厂家后台或者数据库服务器操作后台注册产品注册账户时自动生成账户用户名和密码,并且所述注册账户用户名和密码可通过厂家后台或者数据库服务器操作后台导出,或者数据库服务器在厂家通过厂家后台或者数据库服务器操作后台指令下自动注册所述产品注册账户,在自动注册产品注册账户的同时,如果厂家要求注册产品注册账户的同时自动填写产品信息,则所述数据库服务器完成在所述产品注册账户登记产品信息,并把所述注册账户和密码导出。

4. 根据权利要求 1 所述的系统,其特征在于:当移动客户端解析表达所述产品注册账户网址的二维码,并将通过所述网址访问数据库服务器并接受数据库服务器反馈的信息时,如果数据库服务允许继续输入所述产品注册账户密码进行登录认证时,在反馈显示页面增设一个输入密码框并将输入字符作为对应产品注册账户密码发送至数据库服务器认证,并接受数据库服务器反馈信息并显示给客户,或者增设一个识别二维码命令按钮,当客户点击按钮时移动客户端将开始解析对应所述产品注册账户密码二维码并将之作为对应产品注册账户密码发送至数据库服务器进行认证,并接受数据库服务器反馈信息并显示给客户。

5. 根据权利要求 1 所述的系统,其特征在于:厂家通过厂家后台或者数据库服务器操作后台在所述数据库服务器中注册的所述产品注册账户中除了允许厂家注册商品信息外,还允许首位凭用户名和密码客户通过移动或者 PC 客户端登入所述产品注册账户并在所述产品注册账户中登记客户信息,即当数据库服务器判断此次登入所述产品注册账户为第一次时,则数据库服务器通过移动客户端或者 PC 客户端显示表单给客户填写客户信息并将所述客户信息保存在所述产品注册账户中,所述客户信息比如姓名、电话号码、家庭住址等,对于所述客户信息是否将被反馈给后来持用户名通过移动客户端或者 PC 客户端访问所述注册账户的客户,或者反馈给后来通过移动客户端解析所述注册账户网址二维码并通过所述网址访问所述注册账户的客户,或者反馈给后来通过移动客户端或者 PC 客户端凭用户名和密码访问所述注册账户的客户由厂家对其设定。

6. 根据权利要求 5 所述的系统,其特征在于:当第一位客户凭所述产品注册账户用户名和密码登入所述产品注册账户时,因主观或者客观因素导致未能完成客户信息的登记,所述数据库服务器记录下客户此次登录信息,比如登陆时间或者登录 IP 地址或者将 IP 地址转化为某省某市等地理位置信息,这些信息将呈现给之后持用户名和密码登入所述产品注册账户或者持用户名访问所述产品注册账户的客户,对于是否再次允许客户通过用户名和密码登入所述产品注册账户进行客户信息登记由厂家通过数据库服务器进行设置。

7. 根据权利要求 1 所述的系统,其特征还在于:在注册产品注册账户时,厂家后台或者数据库服务器操作后台亦用于根据已做好的条形码或者二维码防伪查询标签通过对应解

码设备读取所述防伪查询标签上的两串字符分别作为所述产品注册账户的用户名和密码发送至数据库服务器保存,所述条形码或者二维码防伪查询标签含有一对条形码或者二维码,或者一个为条形码一个为二维码,所述二维码或者条形码为可以作为所述产品注册账户的用户名和密码的字符采用条形码或者二维码编码设备编成。

8. 根据权利要求 1 所述的系统,其特征还在于:所述数据库服务器还可以接受被授权用户在被约束的条件下通过被允许操作权修改所述产品注册账户用户名和密码,所述约束条件比如所述被授权用户通过输入正确的用户名和密码第一次登入所述产品注册账户且所述产品注册账户在此之前还未被其他用户凭用户名和密码登入,那么所述被授权用户可以修改该所述注册账户的用户名或密码。

9. 根据权利要求 1 所述的系统,其特征在于:所述数据库服务器还接受被授权用户登陆所述数据库服务器凭借所述产品注册账户用户名就可以在所述产品注册账户登记所述产品注册账户对应的产品的物流信息,比如何时到达何地,何时发往某地,所述物流信息将反馈给通过所述产品注册账户用户名查询所述产品注册账户的客户。

10. 根据权利要求 1 所述的系统,其特征在于:所述数据库服务器还根据厂家在所述产品注册账户中登记的商品过期日期在所述过期日期时关闭或者注销所述产品注册账户或者根据厂家对所述产品注册账户设定关闭或者注销时间关闭或者注销所述产品注册账户。

一种产品防伪查询系统

技术领域

[0001] 本发明涉及一种产品防伪查询系统。

背景技术

[0002] 随着科学技术的发展,仿冒技术越来越先进,与正品一模一样的仿冒品流向市场干扰了正常的市场秩序,损害了正品公司的利益的同时也给消费者带来了甚至巨大的损失,例如,市场上化妆品,而目前常用的激光、纹理防伪技术消费者难以辨认是否为唯一,这非常容易被假冒者找到漏洞(例如在消费者不明白其中原理的情况下,采用欺骗手段将带有激光的标志反复印制在多个假冒产品上),导致消费者经常被假冒产品所欺骗,这些防伪方法存在极大的安全隐患,因此未能起到真正的防伪作用,因此,提供一种对消费者来说易于分辨的产品防伪方法实属必要。再者,目前单一性的数码防伪技术,由于缺乏足够的安全技术,若不法分子对服务器进行递归性输入所谓的唯一密码,那么有极大可能出现这样的情况,就是产品还未售出时,产品所对应的唯一密码已被验证,造成消费者首次输入密码验证时,显示该产品已被售出,另外,如果消费买到正品产品而不查询防伪,那么防伪查询标签丢出去被不法分子检获再用此防伪查询标签贴在假货上,这让正品厂家蒙受不白之冤,给企业带来莫大损失。本发明技术借助互联网(包括移动互联网)技术,克服了上述种种缺点,使防伪技术便利于人们的同时大大地提高了防伪技术的安全性。

发明内容

[0003] 1. 一种产品的防伪系统,包括数据库服务器、移动客户端或者 PC 客户端、厂家后台或者数据库服务器操作后台;其中,数据库服务器用于提供厂家通过厂家后台或者数据库服务器操作后台在数据库服务器中注册产品注册账户以及用于存储厂家通过厂家后台或者数据库服务器操作后台在数据库服务器注册产品注册账户的用户名和密码且对存储的密码进行加密以及用于存储厂家通过厂家后台或者数据库服务器操作后台在所述产品注册账户里登记的产品信息或者厂家信息,以及接受移动客户端或者 PC 客户端发送的所述产品注册账户的用户名和密码请求登入认证并且在认证正确的情况下,除了反馈给移动客户端或者 PC 客户端厂家在所述产品注册账户里登记的产品信息或者厂家信息外,如果这是第一次认证成功,则反馈给移动客户端或者 PC 客户端所查询产品为全新正品信息或者所查询次数为第一次,如果这是第二次或以上次数认证成功,则反馈给移动客户端或者 PC 客户端所述产品注册账户已被激活的信息,所述激活的信息即让客户清楚所述产品注册账户在其之前已被登录,或者提示客户所查询产品涉嫌假冒伪劣的信息,厂家可以通过所述数据库服务器设定当所述产品注册账户已被激活则拒绝提供密码输入认证,以及接受移动客户端或者 PC 客户端发送的所述产品注册账户用户名进行查询所述产品注册账户认证,并且在认证成功的情况下,反馈给移动客户端或者 PC 客户端厂家已在所述产品注册账户里登记的产品信息或者厂家信息或者所述产品注册账户是否已被激活信息或者提醒客户输入账户密码进行下一步认证,如果认证用户名或者密码不正确,则反馈给移动客户端

或者 PC 客户端所查询产品涉嫌假冒伪劣或者提示客户确认正确后再输入,如果所述产品注册账户允许客户通过所述产品注册账户用户名和密码登入所述产品注册账户并登记客户个人信息,则所述数据库服务器还调出客户信息登记表反馈给移动客户端或者 PC 客户端并且接受移动客户端或者 PC 客户端发送客户登记的个人信息并保存在所述产品注册账户中,当移动客户端或者 PC 客户端发送所述产品注册账户的用户名查询注册账户认证请求或者发送所述注册账户的用户名和密码请求登入认证且都正确的情况下,所述个人信息是否反馈给移动客户端或者 PC 客户端由厂家进行设定;

[0004] 移动客户端接用于接受客户输入所述产品注册账户用户名并将所述用户名发送至数据库服务器请求查询注册账户认证并接受数据库服务器反馈的信息并显示给客户以及用于接受客户输入所述产品注册账户用户名和密码并将所述用户名和密码发送至数据库服务器请求登入所述产品注册账户认证并接受数据库服务器反馈的信息并显示给客户,或者用于解析表达所述产品注册账户网址的二维码,并将通过所述网址访问数据库服务器中的所述产品注册账户并接受数据库服务器反馈的信息,所述产品注册账户网址即通过该网址即可访问所述产品注册账户查看厂家已在所述产品注册账户登记的产品信息或者所述注册账户是否已被激活信息,此操作与通过移动客户端或者 PC 客户端通过输入所述产品注册账户用户名查询所述产品注册账号所获取的结果等同,或者用于解析表达所述产品注册账户用户名和密码的二维码或条形码,并将所述产品注册账户用户名和密码发送至数据库服务器请求登入认证并接受数据库服务器反馈的信息并显示给客户,或者用于解析表达所述产品注册账户用户名的二维码或条形码,并将所述产品注册账户用户名发送至数据库服务器请求查询所述产品注册账户认证并接受数据库服务器反馈的信息并显示给客户,如果所述产品注册账户允许客户通过所述产品注册账户用户名和密码登入所述产品注册账户并登记客户个人信息,则所述移动客户端还用于接受客户登记个人信息并发送至所述数据库服务器。

[0005] PC 客户端用于接受客户输入所述产品注册账户用户名并将所述用户名发送至数据库服务器查询所述产品注册账户认证请求并接受数据库服务器反馈的信息并显示给客户以及用于接受客户输入所述产品注册账户用户名和密码并将所述用户名和密码发送至数据库服务器请求登入认证并接受数据库服务器反馈的信息并显示给客户,如果所述产品注册账户允许客户通过所述产品注册账户用户名和密码登入所述产品注册账户并登记客户个人信息,则所述 PC 客户端还用于接受客户登记个人信息并发送至所述数据库服务器;

[0006] 厂家后台或者数据库服务器操作后台用于向数据库服务器注册所述产品注册账户并将所述产品注册账户的用户名和密码导出来,并在所述产品注册账户登记产品信息或者厂家信息,所述产品注册账户的用户名和密码人为生成或者随机生成,获取用户名、密码和登记厂家信息或者产品信息哪个优先执行都可以。

[0007] 所述系统还包括打印设备,所述打印设备将接受厂家后台或者数据库服务器操作后台输出的所述产品注册账户用户名和密码并将其打印出来,如果将所述产品注册账户用户名和密码用条形码或二维码表示,则所述系统增加条形码或二维码编码设备或者在所述厂家后台或者数据库服务器操作后台安装条形码或二维码编码软件,所述编码设备或者条形码或二维码编码软件将表达出所述产品注册账户用户名和密码的条形码或者二维码输入打印设备,并将其打印出来,或者如果将查询所述产品注册账户的网址采用二维码表示

时,将查询所述产品注册账户的网址输入二维码编码设备或者条形码或二维码编码软件,并将表达成的二维码输入打印设备并将其打印出来,所述查询产品注册账户网址即为通过该网址即可访问所述产品注册账户查看厂家已在所述产品注册账户登记的商品信息以及所述产品注册账户是否已被激活信息或者客户已登记的个人信息。

[0008] 数据库服务器还用于,在厂家通过厂家后台或者数据库服务器操作后台注册产品注册账户时自动生成账户用户名和密码,并且所述注册账户用户名和密码可通过厂家后台或者数据库服务器操作后台导出,或者数据库服务器在厂家通过厂家后台或者数据库服务器操作后台指令下自动注册所述产品注册账户,在自动注册产品注册账户的同时,如果厂家要求注册产品注册账户的同时自动填写产品信息,则所述数据库服务器完成在所述产品注册账户登记产品信息,并把所述注册账户和密码导出。

[0009] 当移动客户端解析表达所述产品注册账户网址的二维码,并将通过所述网址访问数据库服务器并接受数据库服务器反馈的信息时,如果数据库服务允许继续输入所述产品注册账户密码进行登录认证时,在反馈显示页面增设一个输入密码框并将输入字符作为对应产品注册账户密码发送至数据库服务器认证,并接受数据库服务器反馈信息并显示给客户,或者增设一个识别二维码命令按钮,当客户点击按钮时移动客户端将开始解析对应所述产品注册账户密码二维码并将之作为对应产品注册账户密码发送至数据库服务器进行认证,并接受数据库服务器反馈信息并显示给客户。

[0010] 厂家通过厂家后台或者数据库服务器操作后台在所述数据库服务器中注册的所述产品注册账户中除了允许厂家注册商品信息外,还允许首位凭用户名和密码客户通过移动或者 PC 客户端登入所述产品注册账户并在所述产品注册账户中登记客户信息,即当数据库服务器判断此次登入所述产品注册账户为第一次时,则数据库服务器通过移动客户端或者 PC 客户端显示表单给客户填写客户信息并将所述客户信息保存在所述产品注册账户中,所述客户信息比如姓名、电话号码、家庭住址等,对于所述客户信息是否将被反馈给后来持用户名通过移动客户端或者 PC 客户端访问所述注册账户的客户,或者反馈给后来通过移动客户端解析所述注册账户网址二维码并通过所述网址访问所述注册账户的客户,或者反馈给后来通过移动客户端或者 PC 客户端凭用户名和密码访问所述注册账户的客户由厂家对其设定。

[0011] 当第一位客户凭所述产品注册账户用户名和密码登入所述产品注册账户时,因主观或者客观因素导致未能完成客户信息的登记,所述数据库服务器记录下客户此次登录信息,比如登陆时间或者登录 IP 地址或者将 IP 地址转化为某省某市等地理位置信息,这些信息将呈现给之后持用户名和密码登入所述产品注册账户或者持用户名访问所述产品注册账户的客户,对于是否再次允许客户通过用户名和密码登入所述产品注册账户进行客户信息登记由厂家通过数据库服务器进行设置。

[0012] 在注册产品注册账户时,厂家后台或者数据库服务器操作后台亦用于根据已做好的条形码或者二维码防伪查询标签通过对应解码设备读取所述防伪查询标签上的两串字符分别作为所述产品注册账户的用户名和密码发送至数据库服务器保存,所述条形码或者二维码防伪查询标签含有一对条形码或者二维码,或者一个为条形码一个为二维码,所述二维码或者条形码为可以作为所述产品注册账户的用户名和密码的字符采用条形码或者二维码编码设备编成。

[0013] 所述数据库服务器还可以接受被授权用户在被约束的条件下通过被允许操作权修改所述产品注册账户用户名和密码,所述约束条件比如所述被授权用户通过输入正确的用户名和密码第一次登入所述产品注册账户且所述产品注册账户在此之前还未被其他用户凭用户名和密码登入,那么所述被授权用户可以修改该所述注册账户的用户名或密码。

[0014] 所述数据库服务器还接受被授权用户登陆所述数据库服务器凭借所述产品注册账户用户名就可以在所述产品注册账户登记所述产品注册账户对应的产品的物流信息,比如何时到达何地,何时发往某地,所述物流信息将反馈给通过所述产品注册账户用户名查询所述产品注册账户的客户。

[0015] 所述数据库服务器还根据厂家在所述产品注册账户中登记的商品过期日期在所述过期日期时关闭或者注销所述产品注册账户或者根据厂家对所述产品注册账户设定关闭或者注销时间关闭或者注销所述产品注册账户。

附图说明

[0016] 图 1 是本发明一种产品防伪查询系统结构示意图;

[0017] 图 2 是防伪产品注册账户注册流程图;

[0018] 图 3 是产品防伪查询流程图。

具体实施方式:

[0019] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0020] 如图示 1 所示,图 1 是本发明一种产品防伪查询系统结构示意图,本发明包括数据库服务器 (1A)、移动客户端 (1B) 或者 PC 客户端 (1C)、厂家后台或者数据库服务器操作后台 (1E),打印设备 (1D),条形码或者二维码编码设备 (1H)。

[0021] 数据库服务器 (1A) 与移动客户端 (1B) 或者 PC 客户端 (1C)、厂家后台或者数据库服务器操作后台 (1E) 通过互联网连接,厂家后台或者数据库服务器操作后台 (1E) 在数据库服务器 (1A) 注册产品注册账户,并把产品注册账户的用户名和密码导出,如果厂家将用户名和密码采用条形码或者二维码 (1G) 表示,则将厂家后台或者数据库服务器操作后台 (1E) 导出的用户名和密码输入在厂家后台或者数据库服务器操作后台 (1E) 安装的条形码或者二维码编码软件,将条形码或者二维码编码软件编码后的用户名和密码 (条形码或者二维码) 输入打印设备 (1D),打印设备 (1D),将所述用户名和密码打印出来制作为防伪查询标签 (1Ga, 1Gb),产品出厂前将所述用户名和密码防伪查询标签 (1Ga, 1Gb) 贴分别贴在商品的外包装和内包装上。如果厂家将查询产品注册账户网址采用二维码表示时,则将所述查询产品注册账户网址输入在厂家或者数据库操作后台安装的二维码软件,将二维码编码软件编码后的产品注册账户网址二维码输入打印设备 (1D),打印设备 (1D),将所述产品注册账户网址打印出来制作为防伪查询标签 (1Fa)。

[0022] 产品进入市场售卖时,客户通过移动客户端 (1B) 或者 PC 客户端 (1C) 根据输入外包装上的用户名或者扫描用户名条形码或者二维码 (1Ga) 或者扫描所述查询产品注册账户网址 (1Fa) 进行初步判定所购买产品是不是正品,如果查询初步判定为正品,且客户

已购买的情况下,再输入内包装上所对应的账户密码或者扫描内包装上的二维码账户密码(1Gb)进行最终判定。

[0023] 如图 2 所示,图 2 是防伪产品注册账户注册流程图,厂家事先通过数据库服务器操作后台在数据库服务器中限定产品注册账户注册模块,比如有产品注册信息注册模块,厂家信息注册模块,厂家通过厂家后台或者数据库服务器操作后台在数据库服务器中注册产品注册账户,所述注册产品注册账户的用户名和密码可由数据库服务器自动生成或者通过厂家后台或者数据库服务器操作中心输入,在获取用户名和密码的同时或之前或之后,厂家在产品注册账户中登记产品信息或者厂家信息。厂家将所述产品注册账户的用户名和密码输入条形码或者二维码编码设备,将得到对应的条形码或者二维码输入打印设备获取产品查询防伪标签或者将所述产品注册账户的用户名和密码直接输入打印设备获得产品防伪查询标签。或者厂家根据产品注册账户的用户名制作出产品注册账户查询网址,将所述查询网址输入二维码编码设备,将得到对应的二维码输入打印设备获取产品注册账户防伪查询标签。

[0024] 将含有用户名在产品防伪查询标签或者产品注册账户防伪查询标签粘贴在产品外包装上,含有产品注册账户密码的标签粘贴在内包装上。

[0025] 如图 3 所示,图 3 是产品防伪查询流程图,在步骤 10 中,消费者揭开产品防伪标签上用户名涂层获取用户名通过 PC 客户端或者移动客户端输入用户名访问产品注册账户或者移动客户端识别解析防伪标签上用二维码表示所述产品注册账户网址访问所述产品注册账户。

[0026] 在步骤 11 中,数据服务器判断用户名或者访问地址是否正确。

[0027] 步骤 12 中如果用户名或者访问地址正确,则显示厂家在所述产品注册账户中登记的商品信息或者厂家信息或者是否所述产品注册账户已被激活。

[0028] 在步骤 13 中,如果所述产品注册账户已被激活,则数据库服务器通知现查询者所查询为假冒伪劣产品,即到步骤 18,如果所述产品注册账户还未被激活,则跳到步骤 14。

[0029] 在步骤 14 中,提示查询者是否输入所述产品注册账户密码进行激活认证,如果查询者选择否,则结束此次查询认证,如果查询者选择继续输入所述产品注册账户密码进行认证激活,则跳到步骤 15 ;

[0030] 步骤 15 中客户揭开密码涂层,在数据库服务器反馈页面上通过移动或者 PC 客户端输入密码。

[0031] 步骤 16 中数据库服务器比对客户验证客户所输入密码是否正确,如果不正确,则跳到步骤 18,如果正确,则到步骤 17。

[0032] 步骤 17 中数据库服务器经过比对客户输入密码正确后,提示客户所查询的产品为正品,并对所述产品注册账户进行激活,以便后来客户凭所述产品注册账户用户名访问所述产品注册账户时清楚所述产品注册账户已被激活,其所查询产品疑为假冒伪劣产品。

[0033] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明。凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

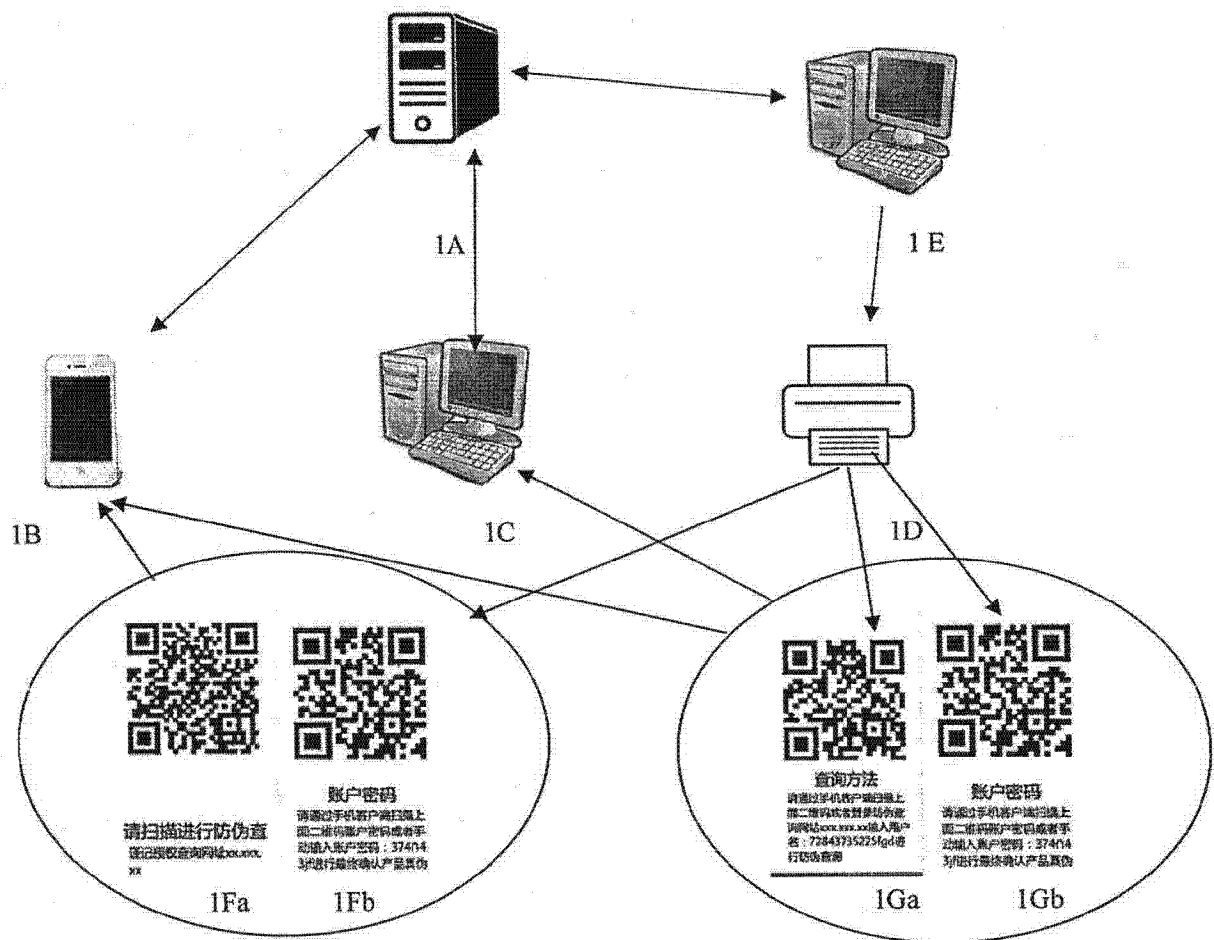


图 1

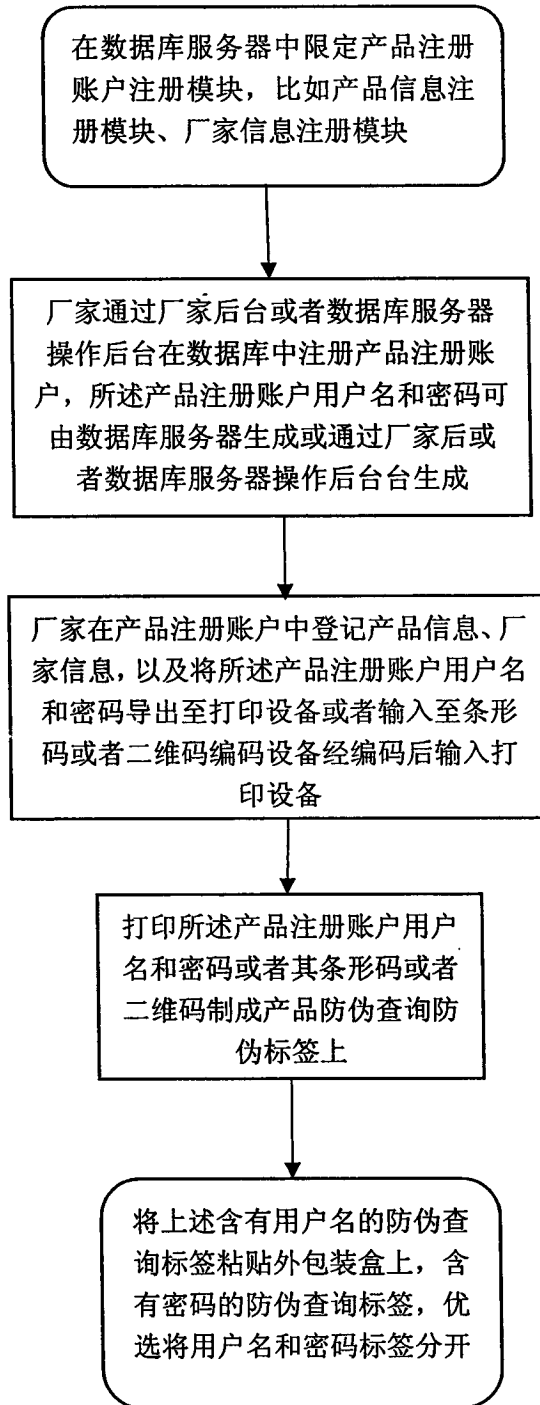


图 2

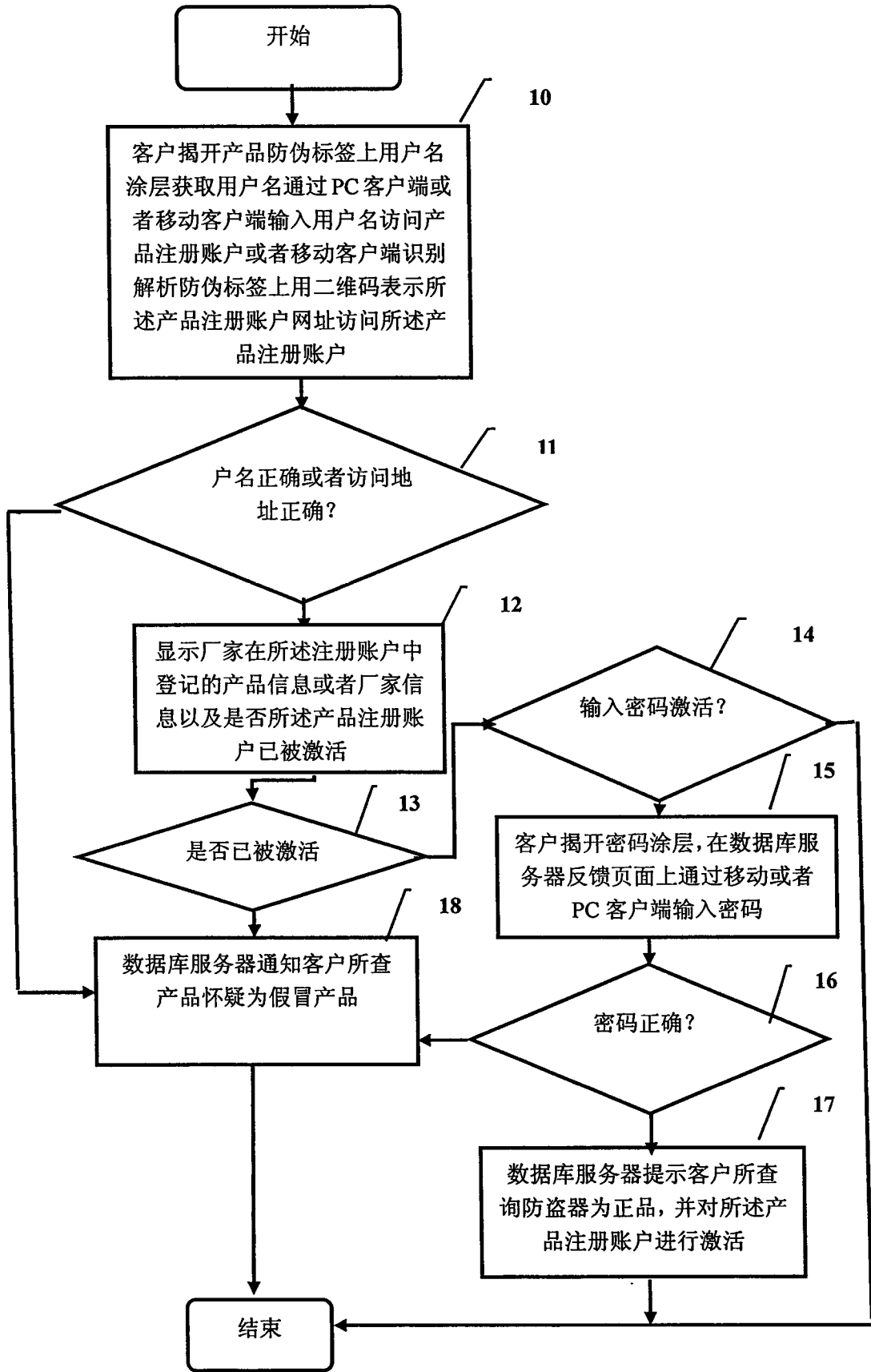


图 3