

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局(43) 国际公布日
2014年3月20日 (20.03.2014) WIPO | PCT

(10) 国际公布号

WO 2014/040479 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) H04W 4/14 (2009.01)
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2013/081942

(22) 国际申请日: 2013年9月4日 (04.09.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210336371.8 2012年9月12日 (12.09.2012) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 郑伟 (ZHENG, Wei); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京派特恩知识产权代理事务所(普通合伙) (CHINA PAT INTELLECTUAL PROPERTY OF-

FICE); 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

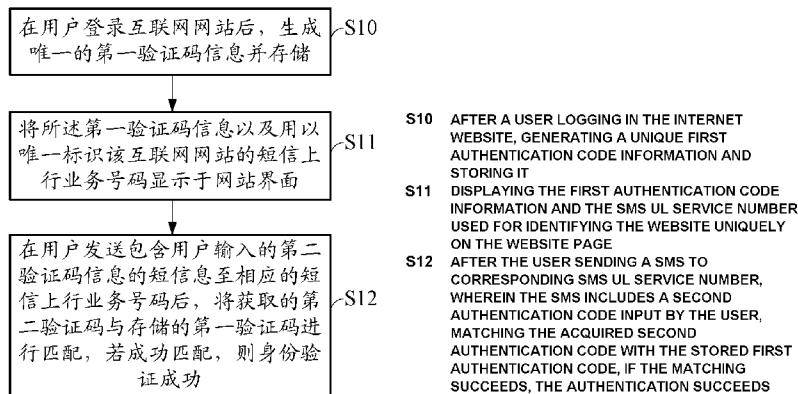
(54) Title: USER IDENTITY AUTHENTICATING METHOD AND DEVICE FOR PREVENTING MALICIOUS HARASSMENT
(54) 发明名称: 防恶意骚扰的用户身份验证方法及装置

图 1 / FIG.1

(57) Abstract: Disclosed is a user identity authenticating method for preventing malicious harassment with a device corresponding to it disclosed. The method comprises: after a user logging in the internet website, generating a unique first authentication code information and storing it; displaying the first authentication code information and the short message (SMS) uplink(UL) service number used for identifying the website uniquely on the website page; after the user sending an SMS to corresponding SMS UL service number, wherein the SMS includes a second authentication code input by the user, matching the acquired second authentication code with the stored first authentication code, if the matching succeeds, the authentication succeeds. The embodiments in the present invention can avoid the possible malicious harassment effectively, thus avoiding the legal risks which the website service provider may confront to some extent, improving the satisfaction of its service. In addition, the increase of processing load and performance influence of the website service provider's server can be avoided in the invention, which are caused by triggering the sending of a large number of authentication codes maliciously.

(57) 摘要:

[见续页]

**本国际公布:**

- 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种防恶意骚扰的用户身份验证方法及装置，所述方法包括：在用户登录互联网网站后，生成唯一的第一验证码信息并存储；将所述第一验证码信息以及用以唯一标识该互联网网站的短信上行业务号码显示于网站界面；在用户发送包含用户输入的第二验证码信息的短信息至相应的短信上行业务号码后，将获取的第二验证码与存储的第一验证码进行匹配，若成功匹配，则身份验证成功。采用本发明可以有效规避可能的恶意骚扰行为，从而一定程度上可以规避互联网服务提供商可能面临的法律风险，提高其业务满意度；另外，采用本发明还能避免恶意触发大量验证码的发送给互联网服务提供商的服务器所造成的处理负荷的增加和性能的影响。

防恶意骚扰的用户身份验证方法及装置

技术领域

本发明涉及计算机互联网络和移动通信技术领域，具体而言，尤其涉及一种防恶意骚扰的用户身份验证方法及装置。

5 背景技术

目前，随着互联网应用的日益发展以及手机的日益普及，越来越多的互联网应用采用手机号码作为登录标识，或采用手机短信息作为消息通知渠道。这种情况下，需要互联网用户提供真实的手机号码，而互联网服务提供商则需要针对用户提供的手机号码信息进行身份验证。

10 现有的手机号码验证方式为：用户通过登录互联网网站并提供一个手机号码，在点击发送验证码按钮后，互联网服务提供商则向该相应的手机号码发送包含验证码信息的短信息，然后用户再在相应有效时间内输入用户手机收到的验证码，并点击提交，从而完成验证过程。

但是，此方法存在这样一个问题，即：如果有其他用户恶意地屡次输入他人的手机号码进行验证，他人会相应地收到多条包含验证码的短信息，此时则会对他人构成一定程度的骚扰，在严重的情况下，可能会引致被骚扰者投诉甚至采取法律行动维权，从而导致互联网服务提供商面临较大的法律风险；另外，当恶意输入手机号码引发互联网服务提供商的服务器需要发送大量验证码时，也会增加服务器的处理负荷，影响服务器的性能。
15 因此，如何提供一种更为有效地可以防止其他用户恶意骚扰的用户身份验证方法便是目前互联网服务提供商亟需解决的一个问题。
20

发明内容

鉴于此，本发明实施例的主要目的在于提供一种防恶意骚扰的用户身

份验证方法及装置。

为了实现本发明实施例的目的，其采用如下技术方案实现：

一方面，本发明实施例提供的一种防恶意骚扰的用户身份验证方法，包括：

5 在用户登录互联网网站后，生成唯一的第一验证码信息并存储；

将所述第一验证码信息以及用以唯一标识该互联网网站的短信上行业务号码显示于网站界面；

在用户发送包含用户输入的第二验证码信息的短信息至相应的短信上行业务号码后，将获取的第二验证码与存储的第一验证码进行匹配，若成10功匹配，则身份验证成功。

优选实施方式下，所述在用户登录互联网网站后，生成唯一的第一验证码信息并存储，包括：

在用户登录互联网网站后，据此生成唯一的会话标识并将其放在网页Cookie中，并生成验证码请求命令；

15 依据该命令，根据会话标识、预设过期时间阈值以及验证码请求命令序列号按照验证码生成算法生成唯一的第一验证码，并将该第一验证码会同对应的会话标识以及过期时间阈值信息进行存储。

优选地实施方式下，所述第一验证码信息显示于网站界面的方式包括：以文字的形式予以显示，或以二维码图像的形式予以显示。

20 优选实施方式下，所述在用户发送包含用户输入的第二验证码信息的短信息至相应的短信上行业务号码后，将获取的第二验证码与存储的第一验证码进行匹配，包括：

在用户依据网站界面的显示信息手动输入第二验证码信息或通过扫描二维码图像输入第二验证码信息之后，发送包含所述第二验证码信息的短25信息至相应的短信上行业务号码；

将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判

判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则身份验证成功。

优选地实施方式下，在执行以上所有步骤之后，所述方法还包括：

向用户手机号码发送身份验证确认短信息；

5 依据获取的用户回复的确认信息，将用户手机号码与本次身份验证的唯一的会话标识进行关联存储，并发送身份验证成功短信息至用户手机号码。

另一方面，本发明实施例提供的一种防恶意骚扰的用户身份验证装置，其包括：

10 验证界面模块，配置为向用户提供互联网网站界面；以及将从验证码生成模块获取的所述第一验证码信息以及用以唯一标识该互联网网站的短信上行业务号码显示于网站界面；

验证码生成模块，配置为在用户登录互联网网站后，生成唯一的第一验证码信息并存储；

15 验证码接收模块，配置为在用户发送包含用户输入的第二验证码信息的短信至相应的短信上行业务号码后，获取用户反馈的第二验证码信息；

验证实施模块，配置为将获取的第二验证码信息与存储的第一验证码进行匹配，若成功匹配，则身份验证成功。

优选实施方式下，所述验证码生成模块还配置为，

20 在用户登录互联网网站后，据此生成唯一的会话标识并将其放在网页Cookie中，并生成验证码请求命令；

依据该命令，根据会话标识、预设过期时间阈值以及验证码请求命令序列号按照验证码生成算法生成唯一的第一验证码，并将该第一验证码会同对应的会话标识以及过期时间阈值信息进行存储。

25 优选地实施方式下，所述验证界面模块所述第一验证码信息显示于网站界面的方式包括：以文字的形式予以显示，或以二维码图像的形式予以

显示。

优选实施方式下，在用户依据网站界面的显示信息手动输入第二验证码信息或通过扫描二维码图像输入第二验证码信息，发送包含所述第二验证码信息的短信至相应的短信上行业务号码之后，所述验证码接收模块
5 获取用户反馈的第二验证码信息；

以及，所述验证实施模块还配置为，将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则身份验证成功。

优选地实施方式下，所述装置还包括：

10 确认短信息发送模块，配置为在身份验证成功之后，向用户手机号码发送身份验证确认短信息；以及在确认短信息接收模块获取到用户回复的确认信息之后，发送身份验证成功短信息至用户手机号码；

确认短信息接收模块，配置为获取用户回复的确认信息，并将用户手机号码与本次身份验证的唯一的会话标识进行关联存储。

15 通过上述本发明实施例的技术方案可以看出，采用本发明实施例，可以有效规避可能的恶意骚扰行为，从而一定程度上可以规避互联网服务提供商可能面临的法律风险，提高其业务满意度；另外，还能避免恶意触发大量验证码的发送给互联网服务提供商的服务器所造成的处理负荷的增加和性能的影响。

20 附图说明

图 1 是本发明实施例提供的一种防恶意骚扰的用户身份验证方法流程示意图；

图 2 是本发明实施例提供的一种防恶意骚扰的用户身份验证装置结构示意图；

25 图 3 是本发明实施例提供的防恶意骚扰的用户身份验证装置工作流程

示意图。

本发明目的的实现、功能特点及优异效果，下面将结合具体实施例以及附图做进一步的说明。

具体实施方式

5 下面结合附图和具体实施例对本发明所述技术方案作进一步的详细描述，以使本领域的技术人员可以更好的理解本发明并能予以实施，但所举实施例不作为对本发明的限定。

如图 1 所示，本发明实施例提供的一种防恶意骚扰的用户身份验证方法，其包括如下步骤：

10 S10、在用户登录互联网网站后，生成唯一的第一验证码信息并存储；
S11、将所述第一验证码信息以及用以唯一标识该互联网网站的短信上行业务号码显示于网站界面，例如，优选实施方式下，所述第一验证码信息显示于网站界面的方式包括：以文字（例如：汉字、英文字母、阿拉伯数字以及其他外文文字等）的形式予以显示，或以二维码图像的形式予以
15 显示；

S12、在用户发送包含用户输入的第二验证码信息的短信息至相应的短信上行业务号码后，将获取的第二验证码与存储的第一验证码进行匹配，若成功匹配，则身份验证成功。

优选实施方式下，在用户登录互联网网站后生成唯一的第一验证码信息并存储的步骤包括：

S101、在用户登录互联网网站后，据此生成唯一的会话标识并将其放在网页 Cookie 中，并生成验证码请求命令；

S102、依据该命令，根据会话标识、预设过期时间阈值以及验证码请求命令序列号按照验证码生成算法生成唯一的第一验证码，并将该第一验证码会同对应的会话标识以及过期时间阈值信息进行存储。
25

优选实施方式下，在用户发送包含用户输入的第二验证码信息的短信至相应的短信上行业务号码后将获取的第二验证码与存储的第一验证码进行匹配的步骤包括：

S121、在用户依据网站界面的显示信息手动输入第二验证码信息或通过扫描二维码图像输入第二验证码信息之后，发送包含所述第二验证码信息的短信息至相应的短信上行业务号码；

S122、将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则身份验证成功。

更为优选地实施方式下，在执行“将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则身份验证成功”步骤之后，所述防恶意骚扰的用户身份验证方法还包括：

S123、向用户手机号码发送身份验证确认短信息；

S124、依据获取的用户回复的确认信息，将用户手机号码与本次身份验证的唯一的会话标识进行关联存储，并发送身份验证成功短信息至用户手机号码。

在所述步骤 S124 中，当用户需要在网站界面查看目前验证过的手机号码，并当用户向服务器后台发送查看请求的时候，该请求会携带与用户手机号码相对应的会话标识，服务器后台根据会话标识在验证码信息保存模块中获取用户手机号码，返回给网站界面予以呈现。

如图 2 所示，本发明实施例还提供了一种防恶意骚扰的用户身份验证装置，其包括：

验证界面模块 101，配置为向用户提供互联网网站界面；以及将从验证码生成模块 102 获取的第一验证码信息以及用以唯一标识该互联网网站的短信上行业务号码显示于网站界面，例如优选实施方式下，所述验证界面

模块 101 将所述第一验证码信息显示于网站界面的方式包括：以文字的形式予以显示，或以二维码图像的形式予以显示；

验证码生成模块 102，配置为在用户登录互联网网站后，生成唯一的第一验证码信息并存储；

5 验证码接收模块 103，配置为在用户发送包含用户输入的第二验证码信息的短信息至相应的短信上行业务号码后，获取用户反馈的第二验证码信息；

验证实施模块 104，配置为将获取的第二验证码信息与存储的第一验证码进行匹配，若成功匹配，则身份验证成功。

10 优选实施方式下，所述验证码生成模块 102 在用户登录互联网网站后生成唯一的第一验证码信息并存储的步骤包括：

(1) 在用户登录互联网网站后，据此生成唯一的会话标识并将其放在网页 Cookie 中，并生成验证码请求命令；

15 (2) 依据该命令，根据会话标识、预设过期时间阈值以及验证码请求命令序列号按照验证码生成算法生成唯一的第一验证码，并将该第一验证码会同对应的会话标识以及过期时间阈值信息进行存储。

优选实施方式下，在用户依据网站界面的显示信息手动输入第二验证码信息或通过扫描二维码图像输入第二验证码信息，发送包含所述第二验证码信息的短信息至相应的短信上行业务号码之后，所述验证码接收模块 20 获取用户反馈的第二验证码信息；

以及，所述验证实施模块 104 将获取的第二验证码与存储的第一验证码进行匹配的步骤包括：

(1) 将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则 25 身份验证成功。

本发明实施例中，更为优选地实施方式下，所述防恶意骚扰的用户身

份验证装置还包括：

确认短信息发送模块 105，配置为在身份验证成功之后，向用户手机号码发送身份验证确认短信息；以及在确认短信息接收模块 106 获取到用户回复的确认信息之后，发送身份验证成功短信息至用户手机号码；

5 确认短信息接收模块 106，配置为获取用户回复的确认信息，并将用户手机号码与本次身份验证的唯一的会话标识进行关联存储。

当用户需要在网站界面查看目前验证过的手机号码，并当用户向服务器后台发送查看请求的时候，该请求会携带与用户手机号码相对应的会话标识，服务器后台根据会话标识在验证码信息保存模块 107 中获取用户手
10 机号码，返回给网站界面予以呈现。

在本发明实施例中，所述防恶意骚扰的用户身份验证装置还包括：

验证码信息保存模块 107，其一方面配置为在用户登录互联网网站后，
存存储第一验证码信息，以及与之对应的会话标识以及过期时间阈值信息；
还配置为记录用户手机号码与对应的会话标识以及过期时间阈值信息的关
15 联关系。

需要说明的是，上述验证界面模块 101、验证码生成模块 102、验证码接收模块 103、验证实施模块 104、确认短信息发送模块 105、确认短信息接收模块 106 可由服务器中的中央处理器 (CPU, Central Processing Unit)、
数字信号处理器 (DSP, Digital Signal Processor) 或可编程逻辑阵列 (FPGA,
20 Field - Programmable Gate Array) 来实现；验证码信息保存模块 107 可由硬
盘或其他硬件存储设备来实现。

为了更进一步说明本发明实施例提供的防恶意骚扰的用户身份验证装置的实施过程，下面结合附图 2 以及图 3 进行详细说明，其具体实施过程如下：

25 步骤 S21：验证界面模块 101 用于向互联网用户提供手机号码验证的网站界面，该验证界面模块 101 依据用户登录互联网网站之后，生成会话标

识，例如所述会话标识一般使用 UUID (Universally Unique Identifier，全局唯一标识符) 值，并将所述会话标识放在网站网页 Cookie 中；

以及，该验证界面模块 101 模块从验证码生成模块 102 获取验证码并显示；其中，所述验证码生成模块 102，在收到验证界面模块 101 发来的获取验证码请求后，根据会话标识，过期时间阈值（例如实施时刻将其可设置为 10 分钟），验证码获取请求序列值（每次请求加 1）按照一定的验证码生成算法生成唯一的验证码，并将此验证码和对应的会话标识、过期时间阈值信息保存于验证码信息保存模块 107 中，其中，所述验证码生成算法可以采用现有技术中提供的各种验证码生成法实现，本文对此不做细述。

步骤 S22：验证界面模块 101 获得验证码后，将验证码以文字的形式显示到网站界面上，在显示验证码的过程中，也可将验证码转换成二维码图像显示到网站界面上。另外，该验证界面模块 101 还提供一个手机短信发送目标号码，即手机短信上行业务号码，互联网服务提供商可以使用该号码接收用户手机发送来的短信内容以及发送者的手机号码。

步骤 S23：用户使用手机将验证界面模块 101 显示的验证码进行输入并将其作为短信内容发送到手机短信发送目标号码，期间，用户可以直接输入验证码作为短信内容，也可以通过具有二维码识别功能的应用软件获取验证码并将其放入短信内容。

步骤 S24：验证码接收模块 103 接收用户手机发送的验证码，并交给验证实施模块 104 进行验证。

步骤 S25：验证实施模块 104 判断验证验证码接收模块 103 收到的验证码在验证码信息保存模块 107 中是否存在，如果存在的话，则判断是否过期，如果不存在或者已过期，则下发短信提示用户重新获取验证码；否则转到步骤 S26。

步骤 S26：为进一步增强安全性，防止有些恶意用户使用某些改号软件发送验证码短信息，可以通过确认短信息发送模块 105 向用户手机号码下

发确认短信。在该实施方式下，采用该技术方案可能一定程度上也会给用户造成骚扰，但是其一定程度上可以更为有效的保障用户的信息安全，并且可以进一步降低互联网服务提供商的法律风险。

步骤 S27：用户使用手机回复确认短信息。

5 步骤 S28：确认短信息接收模块 106 收到用户的确认短信息之后，在验证码信息保存模块 107 中，将用户手机号码通过验证码与相应的会话标识进行关联。

步骤 S29：确认短信息发送模块 105 下发反馈短信息，以提示用户身份验证成功。

10 步骤 S210：用户在网站界面查看目前验证过的手机号码时，在用户向服务器后台发送查看请求的时候，其查看请求带有相应的会话标识，服务器后台根据会话标识在验证码信息保存模块 107 中获取相应的手机号码，并返回至网站界面，以供用户查看。

步骤 S211：结束。

15 以上所述仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

1、一种防恶意骚扰的用户身份验证方法，包括：

在用户登录互联网网站后，生成唯一的第一验证码信息并存储；

将所述第一验证码信息以及用以唯一标识该互联网网站的短信上行

5 业务号码显示于网站界面；

在用户发送包含用户输入的第二验证码信息的短信息至相应的短信
上行业务号码后，将获取的第二验证码与存储的第一验证码进行匹配，
若成功匹配，则身份验证成功。

2、如权利要求 1 所述的防恶意骚扰的用户身份验证方法，其中，所

10 述在用户登录互联网网站后，生成唯一的第一验证码信息并存储，包括：

在用户登录互联网网站后，据此生成唯一的会话标识并将其放在网
页 Cookie 中，并生成验证码请求命令；

依据该命令，根据会话标识、预设过期时间阈值以及验证码请求命
令序列号按照验证码生成算法生成唯一的第一验证码，并将所述第一验
证码会同对应的会话标识以及过期时间阈值信息进行存储。

3、如权利要求 2 所述的防恶意骚扰的用户身份验证方法，其中，所
述第一验证码信息显示于网站界面的方式包括：以文字的形式予以显示，
或以二维码图像的形式予以显示。

4、如权利要求 1 至 3 任一项所述的防恶意骚扰的用户身份验证方法，

20 其中，所述在用户发送包含用户输入的第二验证码信息的短信息至相应
的短信上行业务号码后，将获取的第二验证码与存储的第一验证码进行
匹配，包括：

在用户依据网站界面的显示信息手动输入第二验证码信息或通过扫
描二维码图像输入第二验证码信息之后，发送包含所述第二验证码信息
25 的短信息至相应的短信上行业务号码；

将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则身份验证成功。

5 5. 如权利要求 4 所述的防恶意骚扰的用户身份验证方法，其中，在执行所有步骤之后，还包括：

向用户手机号码发送身份验证确认短信息；

依据获取的用户回复的确认信息，将用户手机号码与本次身份验证的唯一的会话标识进行关联存储，并发送身份验证成功短信息至用户手机号码。

10 6. 一种防恶意骚扰的用户身份验证装置，包括：

验证界面模块，配置为向用户提供互联网网站界面；以及将从验证码生成模块获取的所述第一验证码信息以及用以唯一标识该互联网网站的短信上行业务号码显示于网站界面；

15 验证码生成模块，配置为在用户登录互联网网站后，生成唯一的第
一验证码信息并存储；

验证码接收模块，配置为在用户发送包含用户输入的第二验证码信息的短信至相应的短信上行业务号码后，获取用户反馈的第二验证码信息；

20 验证实施模块，配置为将获取的第二验证码信息与存储的第一验证码进行匹配，若成功匹配，则身份验证成功。

7. 如权利要求 6 所述的防恶意骚扰的用户身份验证装置，其中，所述验证码生成模块还配置为，

在用户登录互联网网站后，据此生成唯一的会话标识并将其放在网页 Cookie 中，并生成验证码请求命令；

25 依据该命令，根据会话标识、预设过期时间阈值以及验证码请求命令序列号按照验证码生成算法生成唯一的第一验证码，并将该第一验证

码会同对应的会话标识以及过期时间阈值信息进行存储。

8、如权利要求 7 所述的防恶意骚扰的用户身份验证装置，其中，所述验证界面模块将所述第一验证码信息显示于网站界面的方式包括：以文字的形式予以显示，或以二维码图像的形式予以显示。

5 9、如权利要求 6 至 8 任一项所述的防恶意骚扰的用户身份验证装置，其中，

在用户依据网站界面的显示信息手动输入第二验证码信息或通过扫描二维码图像输入第二验证码信息，发送包含所述第二验证码信息的短信息至相应的短信上行业务号码之后，所述验证码接收模块获取用户反馈的第二验证码信息；
10

以及，所述验证实施模块还配置为，将所述第二验证码与存储的第一验证码进行匹配，若匹配成功，则判断用户身份验证持续时间是否超过过期时间阈值，若在有效期内，则身份验证成功。

10 10、如权利要求 9 所述的防恶意骚扰的用户身份验证装置，其中，
15 所述装置还包括：

确认短信息发送模块，配置为在身份验证成功之后，向用户手机号码发送身份验证确认短信息；以及在确认短信息接收模块获取到用户回复的确认信息之后，发送身份验证成功短信息至用户手机号码；

确认短信息接收模块，配置为获取用户回复的确认信息，并将用户
20 手机号码与本次身份验证的唯一的会话标识进行关联存储。

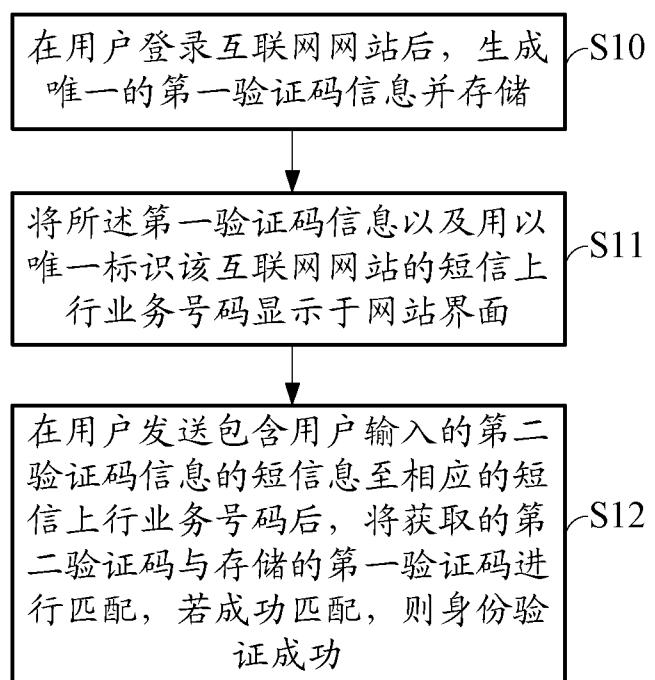


图 1

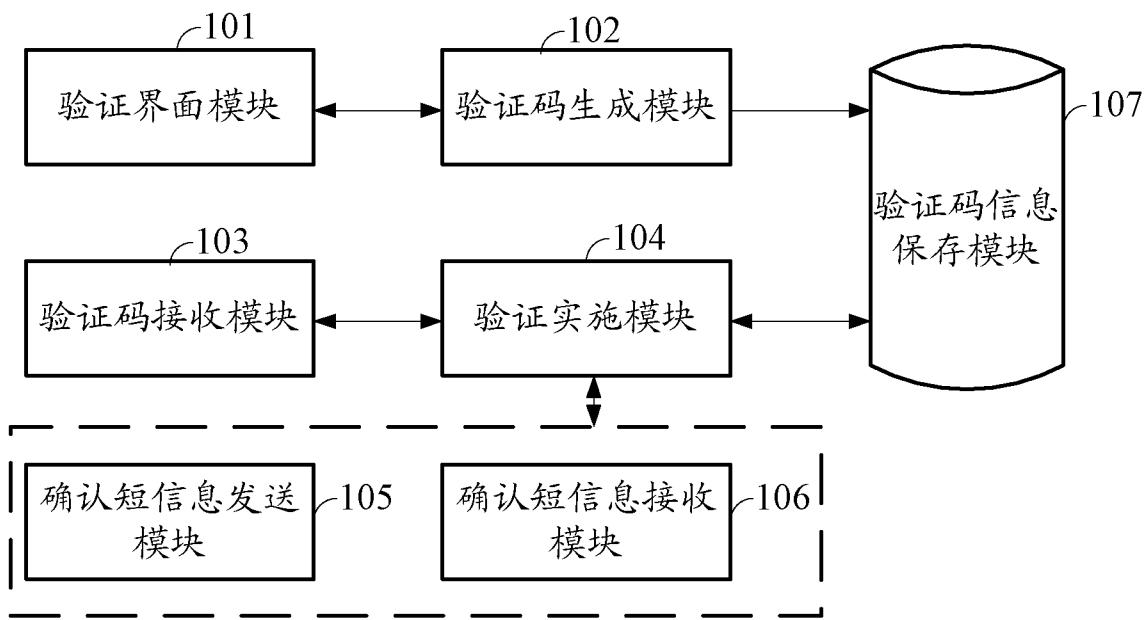


图 2

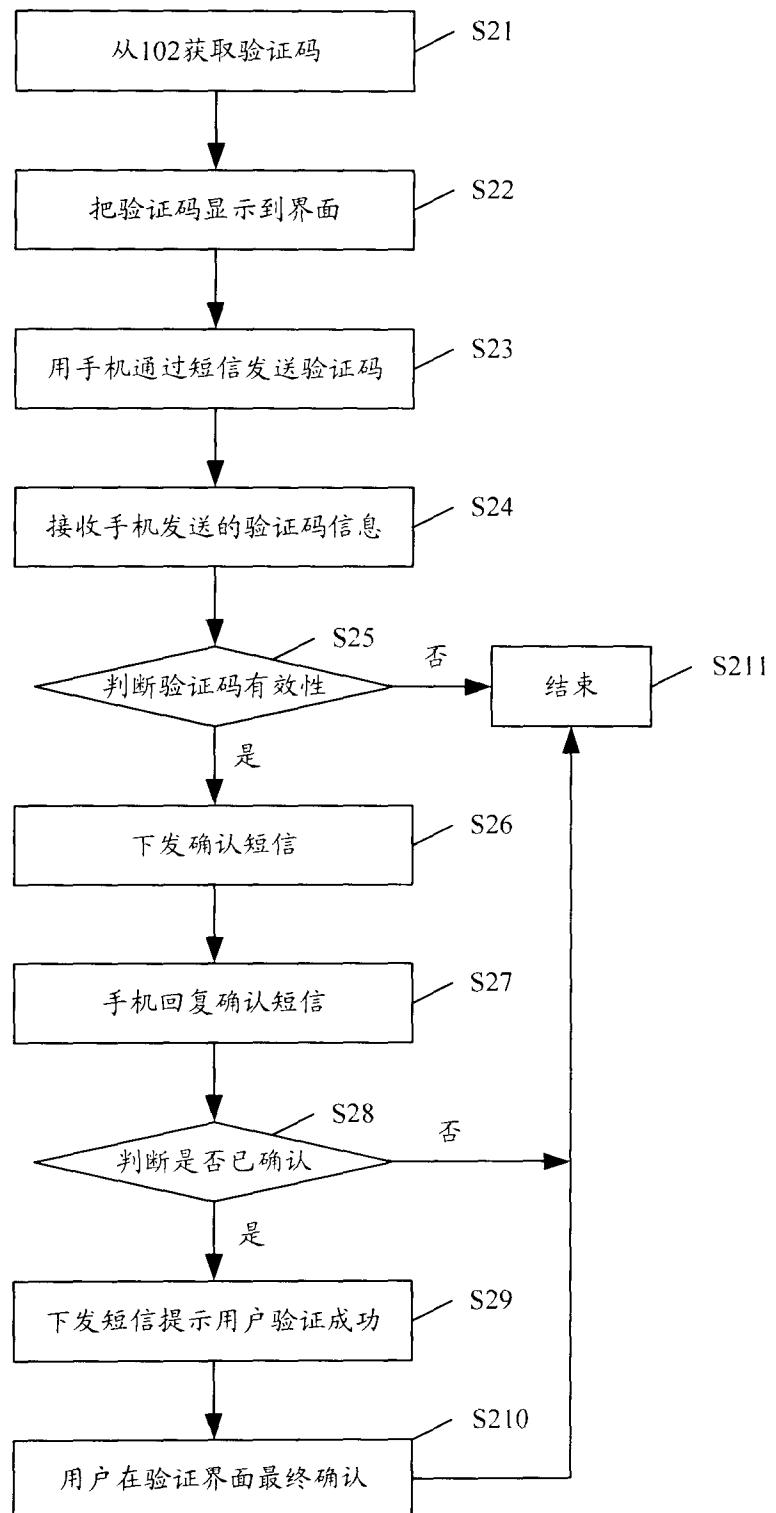


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/081942

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W, H04Q, H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: mobile, number, account, identif+, authenticat+, password, verify, service provider, special service number, access number, SMS, dynamic, match, code

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101087193 A (MA, Jun) 12 December 2007 (12.12.2007) description, page 1, line 3 to page 3, line 2, claim 1	1-10
A	CN 101771684 A (HAN, Yan) 07 July 2010 (07.07.2010) the whole document	1-10
A	CN 1394032 A (SHENZHEN QINGHUA SHENXUN SCIENCE & TECHNOLOGY DEVELOPMENT CO., LTD.) 29 January 2003 (29.01.2003) the whole document	1-10
A	CN 1784063 A (HUAWEI TECHNOLOGIES CO., LTD.) 07 June 2006 (07.06.2006) the whole document	1-10

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 17 November 2013 (17.11.2013)	Date of mailing of the international search report 12 December 2013 (12.12.2013)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Kai Telephone No. (86-10) 62413305

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/081942

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101087193 A	12.12.2007	None	
CN 101771684 A	07.07.2010	None	
CN 1394032 A	29.01.2003	None	
CN 1784063 A	07.06.2006	None	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/081942

CLASSIFICATION OF SUBJECT MATTER:

H04L 9/32 (2006.01) i

H04L 29/06 (2006.01) i

H04W 4/14 (2009.01) i

A. 主题的分类

见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L, H04W, H04Q, H04M

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT,CNKI,WPI,EPODOC: 手机号码, 服务提供商, 接入号码, 特服号, 短消息, 匹配, 动态, 口令, 验证码, 帐号, 验证, 认证, 身份, 字符, 短信, 密码, 身份认证, 身份验证, mobile, number, account, identif+, authenticat+, password, verify

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN101087193A(骏马)12.12月 2007(12.12.2007) 说明书第 1 页第 3 行-第 3 页第 2 行, 权利要求 1	1-10
A	CN101771684A(韩燕)07.7月 2010(07.07.2010) 全文	1-10
A	CN1394032A(深圳市清华深讯科技发展有限公司)29.1月 2003(29.01.2003) 全文	1-10
A	CN1784063A(华为技术有限公司)07.6月 2006(07.06.2006) 全文	1-10

 其余文件在 C 栏的续页中列出。 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

17.11月 2013(17.11.2013)

国际检索报告邮寄日期

12.12月 2013 (12.12.2013)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局
中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

李凯

电话号码: (86-10) 62413305

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/081942

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101087193A	12.12.2007	无	
CN101771684A	07.07.2010	无	
CN1394032A	29.01.2003	无	
CN1784063A	07.06.2006	无	

主题的分类:

H04L 9/32 (2006.01)i

H04L 29/06 (2006.01)i

H04W 4/14 (2009.01)i