



(12) 发明专利申请

(10) 申请公布号 CN 102905052 A

(43) 申请公布日 2013.01.30

(21) 申请号 201210430805.0

(22) 申请日 2012.11.01

(71) 申请人 苏州佳世达电通有限公司

地址 215011 江苏省苏州市高新区珠江路
169 号

(72) 发明人 申如松

(74) 专利代理机构 北京康信知识产权代理有限
责任公司 11240

代理人 吴贵明 张永明

(51) Int. Cl.

H04N 1/44 (2006.01)

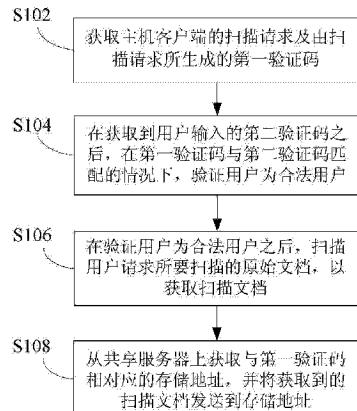
权利要求书 2 页 说明书 10 页 附图 4 页

(54) 发明名称

扫描方法、系统及扫描仪

(57) 摘要

本发明公开了一种扫描方法、系统及扫描仪。其中，该方法包括：获取主机客户端的扫描请求及由扫描请求所生成的第一验证码；在获取到用户输入的第二验证码之后，在第一验证码与第二验证码匹配的情况下，验证用户为合法用户；在验证用户为合法用户之后，扫描用户请求扫描的原始文档，以获取扫描文档；从共享服务器上获取与第一验证码相对应的存储地址，并将获取到的扫描文档发送到存储地址；其中，在获取到由扫描请求所生成的第一验证码之后，将第一验证码发送到共享服务器，以创建第一验证码与存储地址的关联关系。通过本发明，在扫描仪端验证为合法用户之后，才可以扫描需要扫描的文档，实现了安全、简便地进行网络扫描的技术效果。



1. 一种扫描方法,其特征在于,包括:

获取主机客户端的扫描请求及由所述扫描请求所生成的第一验证码;

在获取到用户输入的第二验证码之后,在所述第一验证码与所述第二验证码匹配的情况下,验证所述用户为合法用户;

在验证所述用户为合法用户之后,扫描所述用户请求扫描的原始文档,以获取扫描文档;

从共享服务器上获取与所述第一验证码相对应的存储地址,并将获取到的所述扫描文档发送到所述存储地址;

其中,在获取到由所述扫描请求所生成的第一验证码之后,将所述第一验证码发送到所述共享服务器,以创建所述第一验证码与所述存储地址的关联关系。

2. 根据权利要求1所述的方法,其特征在于,获取主机客户端的扫描请求及由所述扫描请求所生成的第一验证码的步骤包括:

获取所述主机客户端输出的扫描请求;

获取由所述主机客户端根据所述扫描请求中的随机码进行计算,而生成的所述第一验证码。

3. 根据权利要求1所述的方法,其特征在于,所述获取主机客户端的扫描请求及由所述扫描请求所生成的第一验证码的步骤包括:

获取所述主机客户端的扫描请求;

获取由扫描仪根据所述扫描请求中的随机码进行计算,而生成的所述第一验证码。

4. 根据权利要求2或3所述的方法,其特征在于,在获取到用户输入的第二验证码之后,在所述第一验证码与所述第二验证码匹配的情况下,验证所述用户为合法用户的步骤包括:

比对所述第二验证码是否与所述第一验证码一致,其中,

在所述第二验证码与所述第一验证码一致的情况下,验证所述用户为合法用户,

在所述第二验证码与所述第一验证码不一致的情况下,验证所述用户为非法用户。

5. 根据权利要求1所述的方法,其特征在于,在获取由所述扫描请求所生成的第一验证码之后,所述方法还包括:

启动计时器开始计时;

当所述计时时间超过阈值的情况下,由所述扫描请求生成的第一验证码失效;

当所述计时时间没有超过阈值的情况下,保存所述第一验证码。

6. 一种扫描系统,其特征在于,包括:

主机客户端,用于发送扫描请求;

扫描仪,与所述主机客户端连接,包括:

第一获取装置,用于获取所述主机客户端的扫描请求及由所述扫描请求所生成的第一验证码;

比较器,与所述第一获取装置连接,用于在获取到用户输入的第二验证码之后,在所述第一验证码与所述第二验证码匹配的情况下,验证所述用户为合法用户;

扫描装置,与所述比较器连接,用于扫描所述用户请求所要扫描的原始文档,以获取扫描文档;

第一发送装置，与所述扫描装置连接，用于从共享服务器上获取与所述第一验证码相对应的存储地址，并将获取到的所述扫描文档发送到所述存储地址；

所述共享服务器，连接于所述主机客户端与所述扫描仪之间，用于根据获取到的所述第一验证码，创建所述第一验证码与所述存储地址的关联关系。

7. 根据权利要求 6 所述的系统，其特征在于，所述主机客户端包括：

第一处理器，用于根据所述扫描请求中的随机码进行计算，以生成所述第一验证码；

第二发送装置，与所述第一处理器连接，用于发送所述扫描请求及生成的所述第一验证码至所述第一获取装置。

8. 根据权利要求 6 所述的系统，其特征在于，所述扫描仪还包括：

第二处理器，与所述第一获取装置连接，用于根据所述扫描请求中的随机码进行计算而生成所述第一验证码，并将所述第一验证码发送至所述第一获取装置。

9. 根据权利要求 6 所述的系统，其特征在于，所述扫描仪还包括：

计时器，与所述第一获取装置连接，用于在执行所述第一获取装置后开始计时；

第三处理器，与所述计时器连接，用于在所述计时时间超过阈值的情况下，所述由所述扫描请求生成的第一验证码失效；

存储器，与所述计时器连接，用于在所述计时时间没有超过阈值的情况下，保存所述第一验证码。

10. 一种扫描仪，其特征在于，包括：

获取装置，用于获取主机客户端的扫描请求及由所述扫描请求所生成的第一验证码；

比较器，用于在获取到用户输入的第二验证码之后，在所述第一验证码与所述第二验证码匹配的情况下，验证所述用户为合法用户；

扫描装置，用于在验证所述用户为合法用户之后，扫描所述用户请求所要扫描的原始文档，以获取扫描文档；

发送装置，用于从共享服务器上获取与所述第一验证码相对应的存储地址，并将获取到的所述扫描文档发送到所述存储地址；

其中，在获取到由所述扫描请求所生成的第一验证码之后，将所述第一验证码发送到所述共享服务器，以创建所述第一验证码与所述存储地址的关联关系。

扫描方法、系统及扫描仪

技术领域

[0001] 本发明涉及扫描领域,具体而言,涉及一种扫描方法、系统及扫描仪。

背景技术

[0002] 在一些带网络功能的MFP(即多功能一体机)的项目中,MFP具备实现网络扫描的软硬件,在一般的网络扫描的方法中,扫描仪访问用户主机时需要通过网络的身份认证,身份认证主要有两种方法:一种是在扫描设备端输入用户的账号和密码,以访问用户主机中的共享目录,但是该方法操作较繁琐,甚至没有图形用户界面(Graphical User Interface,GUI)或键盘供用户输入密码,对此身份认证的改进方法是将用户名或密码一次性设定在MFP或扫描设备中,但这样又带来了缺乏安全性的问题,并且用户修改密码后,仍有访问权限或管理不便的问题;另一种方法是在MFP或扫描设备中,记录一个特定的账号和密码,此密码可访问用户主机上某一个特定的目录,所有的文档被扫描到同一个文件夹中,不同的用户自行到该文件夹中搜寻各自扫描的文档,这种方法由于用户名和密码可能长时间不会更改,也存在安全隐患的问题,另外服务器上共享的文件夹可以供不同用户查看,也不安全,这种操作方法还有一种改进方法,就是在MFP端输入用户名、密码以及共享的文件夹路径后,开始扫描,扫描完毕后关闭共享,清除用户名、密码等。由上可见,现有的在网络上扫描文档的方法存在安全隐患。

[0003] 针对现有技术中利用网络扫描文档的方法具有安全隐患的问题,目前尚未提出有效的解决方案。

发明内容

[0004] 针对相关技术中利用网络扫描文档的方法具有安全隐患的问题,目前尚未提出有效的解决方案,为此,本发明的主要目的在于提供一种扫描方法、系统及扫描仪,以解决上述问题。

[0005] 为了实现上述目的,根据本发明的一个方面,提供了一种扫描方法,该方法包括:获取主机客户端的扫描请求及由扫描请求所生成的第一验证码;在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户;在验证用户为合法用户之后,扫描用户请求扫描的原始文档,以获取扫描文档;从共享服务器上获取与第一验证码相对应的存储地址,并将获取到的扫描文档发送到存储地址;其中,在获取到由扫描请求所生成的第一验证码之后,将第一验证码发送到共享服务器,以创建第一验证码与存储地址的关联关系。

[0006] 进一步地,获取主机客户端的扫描请求及由扫描请求所生成的第一验证码的步骤包括:获取主机客户端输出的扫描请求;获取由主机客户端根据扫描请求中的随机码进行计算,而生成的第一验证码。

[0007] 进一步地,获取主机客户端的扫描请求及由扫描请求所生成的第一验证码的步骤包括:获取主机客户端的扫描请求;获取由扫描仪根据扫描请求中的随机码进行计算,而

生成的第一验证码。

[0008] 进一步地,在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户的步骤包括:比对第二验证码是否与第一验证码一致,其中,在第二验证码与第一验证码一致的情况下,验证用户为合法用户,在第二验证码与第一验证码不一致的情况下,验证用户为非法用户。

[0009] 进一步地,在获取由扫描请求所生成的第一验证码之后,方法还包括:启动计时器开始计时;当计时时间超过阈值的情况下,由扫描请求生成的第一验证码失效;当计时时间没有超过阈值的情况下,保存第一验证码。

[0010] 为了实现上述目的,根据本发明的另一方面,提供了一种扫描系统,该系统包括:主机客户端,用于发送扫描请求;扫描仪,与主机客户端连接,包括:第一获取装置,用于获取主机客户端的扫描请求及由扫描请求所生成的第一验证码;比较器,与第一获取装置连接,用于在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户;扫描装置,与比较器连接,用于扫描用户请求所要扫描的原始文档,以获取扫描文档;第一发送装置,与扫描装置连接,用于从共享服务器上获取与第一验证码相对应的存储地址,并将获取到的扫描文档发送到存储地址;共享服务器,连接于主机客户端与扫描仪之间,用于根据获取到的第一验证码,创建第一验证码与存储地址的关联关系。

[0011] 进一步地,主机客户端包括:第一处理器,用于根据扫描请求中的随机码进行计算,以生成第一验证码;第二发送装置,与第一处理器连接,用于发送扫描请求及生成的第一验证码至第一获取装置。

[0012] 进一步地,扫描仪还包括:第二处理器,与第一获取装置连接,用于根据扫描请求中的随机码进行计算而生成第一验证码,并将第一验证码发送至第一获取装置。

[0013] 进一步地,扫描仪还包括:计时器,与第一获取装置连接,用于在执行第一获取装置后开始计时;第三处理器,与计时器连接,用于在计时时间超过阈值的情况下,由扫描请求生成的第一验证码失效;存储器,与计时器连接,用于在计时时间没有超过阈值的情况下,保存第一验证码。

[0014] 为了实现上述目的,根据本发明的另一方面,提供了一种扫描仪,该扫描仪包括:获取装置,用于获取主机客户端的扫描请求及由扫描请求所生成的第一验证码;比较器,用于在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户;扫描装置,用于在验证用户为合法用户之后,扫描用户请求所要扫描的原始文档,以获取扫描文档;发送装置,用于从共享服务器上获取与第一验证码相对应的存储地址,并将获取到的扫描文档发送到存储地址;其中,在获取到由扫描请求所生成的第一验证码之后,将第一验证码发送到共享服务器,以创建第一验证码与存储地址的关联关系。

[0015] 通过本发明提供的扫描方法、系统及扫描仪,用户通过主机客户端发送扫描请求,在扫描仪端验证为合法用户之后,才可以扫描需要扫描的文档,增加了扫描的安全性,并且在扫描仪获取到扫描文档之后,扫描仪通过共享服务器获取存储扫描文档的地址,之后才将扫描文档发送到用户设定的存储地址,而不是直接将扫描文档发送到本机,解决了现有技术中利用网络扫描文档的方法具有安全性隐患且操作繁琐的问题,进而实现了安全、简便地进行网络扫描的技术效果。

附图说明

- [0016] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:
- [0017] 图 1 是根据本发明实施例的扫描系统的结构示意图;
- [0018] 图 2 是根据本发明实施例的扫描方法的流程图;
- [0019] 图 3 是根据图 2 所示的扫描方法的第一实施例的方法流程图;
- [0020] 图 4 是根据图 2 所示的扫描方法的第二实施例的方法流程图;
- [0021] 图 5 是根据图 2 所示的扫描方法的第三实施例的方法流程图;以及
- [0022] 图 6 是根据本发明实施例的扫描仪的结构示意图。

具体实施方式

[0023] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

[0024] 图 1 是根据本发明实施例的扫描系统的结构示意图。如图 1 所示,扫描系统包括主机客户端 1、扫描仪 3 以及共享服务器 5。主机客户端 1 用于发送扫描请求;扫描仪 3 与主机客户端 1 连接,且扫描仪 3 包括第一获取装置 31、比较器 33、扫描装置 35 以及第一发送装置 37。第一获取装置 31 用于获取主机客户端 1 发出的扫描请求及由扫描请求所生成的第一验证码。比较器 33 与第一获取装置 31 连接,用于在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户。扫描装置 35 与比较器 33 连接,用于扫描用户请求所要扫描的原始文档,以获取扫描文档。第一发送装置 37 与扫描装置 35 连接,用于从共享服务器 5 上获取与第一验证码相对应的存储地址,并将获取到的扫描文档发送到存储地址。共享服务器 5 连接于主机客户端 1 与扫描仪 3 之间,用于根据获取到的第一验证码,创建第一验证码与存储地址的关联关系。

[0025] 采用本发明的扫描系统,通过扫描仪 3 中的第一获取装置 31 获取到主机客户端 1 发送的扫描请求及由扫描请求所生成的第一验证码,然后扫描仪 3 中的比较器 33 在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户,之后通过扫描仪 3 中的扫描装置 35 扫描用户请求所要扫描的原始文档,在获取到扫描文档之后,扫描仪 3 中的第一发送装置 37 从共享服务器 5 上获取与第一验证码相对应的存储地址,并将获取到的扫描文档发送到存储地址,其中,共享服务器 5 连接于主机客户端 1 与扫描仪 3 之间,可以根据获取到的第一验证码,创建第一验证码与存储地址的关联关系。通过本发明提供的扫描系统,用户通过主机客户端 1 发送扫描请求,在扫描仪端验证为合法用户之后,才可以在扫描仪 3 扫描用户需要扫描的文档,增加了扫描的安全性,并且在扫描仪 3 获取到扫描文档之后,通过共享服务器 5 获取用户设定的存储地址,而不是直接将扫描文档发送到本机,解决了现有技术中利用网络扫描文档的方法具有安全性隐患的问题,进而实现了安全、简便地进行网络扫描的技术效果。

[0026] 其中,第一获取装置 31 获取到的第一验证码可以是主机客户端 1 生成的,然后发送给扫描仪 3,也可以是扫描仪 3 根据扫描请求自己而生成的。主机客户端 1 可以是个人电脑、智能手机等终端,存储地址可以是主机客户端 1 上的文件,也可以是用户指定的一个特定的 Email 地址、云端存储地址或网络打印机等。具体地,验证码可以是数字码,共享服务

器 5 可以是 EWS 等 web 程序。在本发明的上述实施例中,不需要将扫描文档扫描到主机客户端 1 上的文件夹,再通过主机客户端 1 发送到其他地方,也不需要在扫描仪 3 上记录或输入云端位置、Email 地址或网络打印机的名称或设定信息,扫描仪 3 通过共享服务器 5 创建的第一验证码与存储地址的关联关系,可以直接得到用户设定的存储地址,实现了安全简便进行网络扫描的效果。

[0027] 具体地,主机客户端 1 还可以包括:第一处理器,用于根据扫描请求中的随机码进行计算,以生成第一验证码;第二发送装置,与第一处理器连接,用于发送扫描请求及生成的第一验证码至第一获取装置 31。其中,主机客户端 1 可以是个人电脑、智能手机等终端。

[0028] 具体地,主机客户端 1 获取用户根据扫描需求发送到主机客户端 1 的扫描请求,主机客户端 1 可以将该扫描请求发送给扫描仪 3 或主机客户端 1 并根据该扫描请求计算而生成第一验证码,然后将该扫描请求及其第一验证码发送给第一获取装置 31。例如,用户可以通过手机向扫描仪 3 发送一个扫描图片的请求,也可以通过手机根据该图片生成一个数字码,并向扫描仪 3 发送一个扫描图片及该数字码。

[0029] 根据本发明的上述实施例,第一验证码还可以采用如下方式生成,例如扫描仪 3 还可以包括第二处理器,第二处理器与第一获取装置 31 连接,用于根据扫描请求中的随机码进行计算,以生成第一验证码。

[0030] 根据本申请的上述实施例,扫描仪 3 还可以包括:计时器,与第一获取装置 31 连接,用于在执行第一获取装置 31 后开始计时;检测装置,与计时器连接,用于在计时时间超过阈值的情况下,由扫描请求生成的第一验证码失效;存储器,与计时器连接,用于在计时时间没有超过阈值的情况下,保存第一验证码。

[0031] 优选地,计时器在执行第一获取装置 31 后开始计时,即在获取由扫描请求所生成的第一验证码之后启动计时器。在启动计时器之后,检测装置在计时器计时时间超过阈值的情况下,使得由扫描请求生成的第一验证码失效;在计时器计时时间没有超过阈值的情况下,由存储器保存第一验证码,以供用户验证身份使用。其中,检测装置使得第一验证码失效的方式有多种,例如可以是删除该第一验证码。阈值可以设定为用户完成一般的扫描操作需要的时间,例如,用户完成扫描需要 180 秒,可以将阈值设定为 180 秒;阈值也可以直接根据检测到的“用户完成扫描”的信号获取,例如检测到的信号表示用户完成扫描,则检测装置使得第一验证码失效。检测装置在计时器计时时间超过阈值的情况下使由扫描请求生成的第一验证码失效,则用户下一次使用该第一验证码进行身份验证的时候不能通过身份验证,从而不能使用扫描功能,进而保证了扫描系统的安全性。

[0032] 根据本申请的上述实施例,共享服务器 5 可以包括:第六获取装置,用于获取第一验证码;第三处理器,用于根据第一验证码,创建第一验证码与存储地址的关联关系。

[0033] 具体地,共享服务器 5 中的第六获取装置获取扫描仪 3 发送的第一验证码,然后根据获取到的第一验证码创建该第一验证码与存储地址的关联关系。扫描仪 3 在获取到扫描文档之后,可以通过第三处理器创建的关联关系,获取到扫描文档的存储地址,然后将扫描文档发送到该存储地址。扫描仪 3 可以根据不同的第一验证码识别不同的用户,然后根据第一验证码与存储地址的关联关系,将不同用户的扫描文档发送到不同的存储地址,不仅能准确完成扫描功能,而且不需要先将扫描文档存储在主机客户端 1 然后再发送到其他地址,也不需要在扫描仪 3 上记录或输入云端地址、邮件地址或网络打印机的名称或设定信

息等操作，扫描仪 3 可以直接根据该关联关系将根据用户请求扫描后的扫描文档发送到用户需要发送的存储地址，安全简便地实现了网络扫描。

[0034] 图 2 是根据本发明实施例的扫描方法的流程图。如图 2 所示该方法包括如下步骤：

[0035] 步骤 S102，获取主机客户端的扫描请求及由扫描请求所生成的第一验证码。其中，主机客户端可以是个人电脑、智能手机等终端。

[0036] 步骤 S104，在获取到用户输入的第二验证码之后，在第一验证码与第二验证码匹配的情况下，验证用户为合法用户。

[0037] 步骤 S106，在验证用户为合法用户之后，扫描用户请求所要扫描的原始文档，以获取扫描文档。

[0038] 步骤 S108，从共享服务器上获取与第一验证码相对应的存储地址，并将获取到的扫描文档发送到存储地址。

[0039] 其中，在获取到由扫描请求所生成的第一验证码之后，将第一验证码发送到共享服务器，以创建第一验证码与存储地址的关联关系。

[0040] 采用本发明的扫描方法，通过获取主机客户端发送的扫描请求及由扫描请求所生成的第一验证码，然后扫描仪在获取到用户输入的第二验证码之后，在第一验证码与第二验证码匹配的情况下，验证用户为合法用户，之后扫描用户请求所要扫描的原始文档，在获取到扫描文档之后，扫描仪从共享服务器上获取与第一验证码相对应的存储地址，并将获取到的扫描文档发送到存储地址，其中，共享服务器可以根据获取到的第一验证码创建第一验证码与存储地址的关联关系。通过本发明提供的扫描方法，用户通过主机客户端发送扫描请求，在扫描仪端验证为合法用户之后，才可以在扫描仪扫描用户需要扫描的文档，增加了扫描的安全性，并且在扫描仪获取到扫描文档之后，通过共享服务器获取用户设定的存储地址，而不是直接将扫描文档发送到本机，解决了现有技术中利用网络扫描文档的方法具有安全性隐患的问题，进而实现了安全、简便地进行网络扫描的技术效果。

[0041] 其中，存储地址可以是主机客户端上的文件夹，也可以是用户指定的一个特定的 Email 地址、云端存储地址或网络打印机等。具体地，验证码可以是数字码，共享服务器可以是 EWS 等 web 程序。在本发明的上述实施例中，不需要将扫描文档扫描到主机客户端上的文件夹，再通过主机客户端发送到其他地方，也不需要在扫描仪上记录或输入云端位置、Email 地址或网络打印机的名称或设定信息，扫描仪通过共享服务器创建的第一验证码与存储地址的关联关系，可以直接得到用户设定的存储地址，实现了安全简便进行网络扫描的效果。

[0042] 根据本发明的扫描方法的实施例，获取主机客户端的扫描请求及由扫描请求所生成的第一验证码的步骤可以包括：获取主机客户端输出的扫描请求；获取由主机客户端根据扫描请求中的随机码进行计算，而生成的第一验证码。

[0043] 具体地，主机客户端获取用户根据扫描需求发送到主机客户端的扫描请求，主机客户端可以将该扫描请求发送给扫描仪或主机客户端根据该扫描请求计算而生成第一验证码，然后将该扫描请求及其第一验证码发送给扫描仪。

[0044] 根据本发明的上述实施例，获取主机客户端的扫描请求及由扫描请求所生成的第一验证码的步骤可以包括：获取主机客户端的扫描请求；获取由扫描仪根据扫描请求中的

随机码进行计算,而生成的第一验证码。

[0045] 具体地,在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户的步骤包括:比对第二验证码是否与第一验证码一致,其中,在第二验证码与第一验证码一致的情况下,验证用户为合法用户,在第二验证码与第一验证码不一致的情况下,验证用户为非法用户。

[0046] 更具体地,在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户的步骤包括:比对第二验证码与主机客户端生成的第一验证码是否一致,其中,在第二验证码与主机客户端生成的第一验证码一致的情况下,验证用户为合法用户;在第二验证码与主机客户端生成的第一验证码不一致的情况下,验证用户为非法用户。

[0047] 另外,在获取到用户输入的第二验证码之后,在第一验证码与第二验证码匹配的情况下,验证用户为合法用户的步骤还可以包括:比对第二验证码是否与扫描仪生成的第一验证码一致,其中,在第二验证码与扫描仪生成的第一验证码一致的情况下,验证用户为合法用户;在第二验证码与扫描仪生成的第一验证码不一致的情况下,验证用户为非法用户。

[0048] 根据本发明的上述实施例,在从获取由扫描请求所生成的第一验证码之后,方法还可以包括:启动计时器开始计时;当计时时间超过阈值的情况下,由扫描请求生成的第一验证码失效;当计时时间没有超过阈值的情况下,保存第一验证码。

[0049] 具体地,在获取由扫描请求所生成的第一验证码之后启动计时器,在启动计时器之后,检测装置在计时器计时时间超过阈值的情况下,使得由扫描请求生成的第一验证码失效;在计时器计时时间没有超过阈值的情况下,由存储器保存第一验证码,以供用户验证身份使用。其中,检测装置使得第一验证码失效的方式有多中,可以是删除该第一验证码。阈值可以设定为用户完成一般的扫描操作需要的时间,例如,用户完成扫描需要 180 秒,可以将阈值设定为 180 秒;阈值也可以直接根据检测到的“用户完成扫描”的信号获取,例如检测到的信号表示用户完成扫描,则检测装置使得第一验证码失效。检测装置在计时器计时时间超过阈值的情况下使由扫描请求生成的第一验证码失效,则用户下一次使用该第一验证码进行身份验证的时候不能通过身份验证,从而不能使用扫描功能,进而保证了扫描系统的安全性。

[0050] 在本申请的上述实施例中,扫描方法可以通过如下步骤实现:主机客户端发送扫描请求至扫描仪,主机客户端或扫描仪根据扫描请求生成第一验证码,并建立第一验证码与主机客户端对应的存储地址的关联关系,在获取用户输入的第二验证码之后,比对第一验证码与第二验证码是否匹配,若第一验证码与第二验证码匹配,则扫描仪扫描用户请求扫描的原始文档,并将获取的扫描文档发送到存储地址,并在扫描完成后删除第一验证码与存储地址的关联关系。

[0051] 图 3 是根据图 2 所示的扫描方法的第一实施例的方法流程图。图 3 示出了利用 EWS(embedded web server) 等 web 程序访问到扫描仪进行扫描的第一方法实施例,在该实施例中包括如下步骤:

[0052] 步骤 S301,打开共享服务器 EWS。即用户进入 EWS 程序的操作环境,通过 EWS 访问扫描仪。其中, EWS 程序即为上述实施例中的共享服务器。

- [0053] 步骤 S302,本机对扫描请求进行处理。其中,本机为主机客户端。
- [0054] 具体地,用户通过本机将扫描请求发送到扫描仪。
- [0055] 步骤 S303,扫描仪发送验证码并显示在 EWS 网页中。
- [0056] 具体地,图 2 中的步骤 S102 可以通过步骤 S302 和 S303 实现:在该实施例中,扫描仪在获取到用户的扫描请求之后,根据该扫描请求生成验证码(即上述实施例中的第一验证码),然后在将第一验证码发送给用户的同时,将第一验证码发送到 EWS 并显示在网页中。
- [0057] 步骤 S304,共享服务器 EWS 临时共享本机目录给扫描仪。
- [0058] 具体地,EWS 程序根据第一验证码创建数字码与目标存储地址的关联关系,并将该关联关系反馈给扫描仪,而本机目录即通过第一验证码创建数字码与目标存储地址的关联关系来生成。
- [0059] 步骤 S305,用户在扫描仪 GUI 中输入验证码。
- [0060] 在该实施例中,步骤 S305 可以实现图 2 中步骤 S104 的通过第一验证码和第二验证码的匹配验证用户为合法用户的过程,具体地,在步骤 S304 之后,用户在扫描仪上扫描文档时,根据扫描仪的提示,在扫描仪 GUI(即扫描仪的图形用户界面)中输入验证码(此处的验证码为上述实施例中的第二验证码),扫描仪进行身份验证,在第一验证码与第二验证码一致的情况下,扫描仪验证用户为合法用户,开始扫描用户请求所要扫描的原始文档,获取到扫描文档。用户在扫描仪上扫描文档时,输入第二验证码,通过身份验证后扫描仪即知道该向哪个本机发送扫描的文档。即使没有 GUI 或数字键的情况下,仅仅通过某些 button 的按键顺序等识别不同的用户。
- [0061] 步骤 S306,扫描仪根据该本机目录扫描文档至与验证码对应的目标存储地址中。
- [0062] 在该实施例中,图 2 中的步骤 S106 和 S108 可以通过步骤 S306 来实现,具体地,扫描仪在验证用户为合法用户之后,扫描用户所要扫描的原始文档,获取到扫描文档,然后根据从 EWS 程序中获取该本机目录即第一验证码与用户存储地址的关联关系,获取到存储地址,直接将扫描文档存储到该存储地址。
- [0063] 步骤 S307,结束扫描,EWS 关闭本机目录共享,然后关闭共享服务器 EWS。
- [0064] 具体地,结束扫描,EWS 关闭本机目录共享,第一验证码时失效,用户可以关闭 EWS。用户扫描完成后本机目录共享关系、第一验证码失效,则用户下一次使用该第一验证码进行身份验证的时候不能通过身份验证,从而不能使用扫描功能,进而保证了扫描系统的安全性。
- [0065] 图 4 是根据图 2 所示的扫描方法的第二实施例的方法流程图。图 4 示出了利用 EWS(embedded web server) 等 web 程序访问到扫描仪进行扫描的第二方法实施例,在该实施例中包括如下步骤:
- [0066] 步骤 S401,打开共享服务器 EWS。即用户进入 EWS 程序的操作环境,通过 EWS 访问扫描仪。其中,EWS 程序即为上述实施例中的共享服务器。
- [0067] 步骤 S402,本机对扫描请求进行处理。
- [0068] 具体地,用户通过本机将扫描请求发送到扫描仪。
- [0069] 步骤 S403,本机发送验证码给扫描仪并显示在共享服务器 EWS 网页中。
- [0070] 具体地,图 2 中步骤 S102 可以通过步骤 S402 和 S403 实现:在该实施例中,用户

通过主机发送扫描请求的同时将根据该扫描请求生成第一验证码发送到扫描仪,而且本机在将第一验证码发送给扫描仪的同时,将第一验证码发送给共享服务器 EWS 并显示在网页中。

[0071] 步骤 S404,共享服务器 EWS 临时共享本机目录给扫描仪。

[0072] 具体地,EWS 程序根据第一验证码创建数字码与目标存储地址的关联关系,并将该关联关系反馈给扫描仪,而本机目录即通过第一验证码创建数字码与目标存储地址的关联关系来生成。

[0073] 步骤 S405,用户在扫描仪 GUI 中输入验证码。

[0074] 在该实施例中,步骤 S405 可以实现图 2 中步骤 S104 的通过第一验证码和第二验证码的匹配验证用户为合法用户的过程,具体地,在步骤 S404 之后,用户在扫描仪上扫描文档时,根据扫描仪的提示,在扫描仪 GUI 中输入验证码(此处的验证码为上述实施例中的第二验证码),扫描仪进行身份验证,在第一验证码与第二验证码一致的情况下,扫描仪验证用户为合法用户,开始扫描用户请求所要扫描的原始文档,获取到扫描文档。用户在扫描仪上扫描文档时,输入第二验证码,通过身份验证后扫描仪即知道该向哪个本机发送扫描的文档。即使没有 GUI 或数字键的情况下,仅仅通过某些 button 的按键顺序等识别不同的用户。

[0075] 步骤 S406,扫描仪根据该本机目录扫描文档至与验证码对应的目标存储地址中。

[0076] 在该实施例中,图 2 中的步骤 S106 和 S108 可以通过步骤 S406 来实现,具体地,扫描仪在验证用户为合法用户之后,扫描用户所要扫描的原始文档,获取到扫描文档,然后根据从 EWS 程序中获取该本机目录即第一验证码与用户存储地址的关联关系,获取到存储地址,直接将扫描文档存储到该存储地址。

[0077] 步骤 S407,结束扫描,共享服务器 EWS 关闭本机目录共享,然后关闭共享服务器 EWS。

[0078] 具体地,结束扫描,EWS 关闭本机目录共享,第一验证码失效,用户可以关闭 EWS。用户扫描完成后本机目录共享关系、第一验证码失效,则用户下一次使用该第一验证码进行身份验证的时候不能通过身份验证,从而不能使用扫描功能,进而保证了扫描系统的安全性。

[0079] 图 5 是根据图 2 所示的扫描方法的第三实施例的方法流程图。图 5 示出了利用 EWS(embedded web server) 等 web 程序访问到扫描仪进行扫描的第三方法实施例,在该实施例中包括如下步骤:

[0080] 步骤 S501,打开共享服务器 EWS。即用户进入 EWS 程序的操作环境,通过 EWS 访问扫描仪。其中,EWS 程序即为上述实施例中的共享服务器。

[0081] 步骤 S502,本机对扫描请求进行处理。

[0082] 具体地,用户通过本机将扫描请求发送到扫描仪。

[0083] 步骤 S503,本机发送验证码给扫描仪并显示在 EWS 网页中。

[0084] 具体地,图 2 中步骤 S102 可以通过步骤 S502 和 S503 实现:在该实施例中,用户通过主机发送扫描请求的同时将根据该扫描请求生成验证码(即上述实施例中的第一验证码)发送到扫描仪,并将第一验证码发送给 EWS 并显示在网页中。

[0085] 步骤 S504,共享服务器 EWS 临时共享本机目录给扫描仪。

[0086] 具体地，EWS 程序根据第一验证码创建数字码与用户设定的云端位置（即上述实施例中的存储地址）的关联关系，并将该关联关系反馈给扫描仪，而本机目录即通过第一验证码创建数字码与目标存储地址的关联关系来生成。。

[0087] 步骤 S505，用户在扫描仪 GUI 中输入验证码。

[0088] 在该实施例中，步骤 S505 可以实现图 2 中步骤 S104 的通过第一验证码和第二验证码的匹配验证用户为合法用户的过程，具体地，在步骤 S504 之后，用户在扫描仪上扫描文档时，根据扫描仪的提示，在扫描仪 GUI 中输入验证码（此处的验证码为上述实施例中的第二验证码），扫描仪进行身份验证，在第一验证码与第二验证码一致的情况下，扫描仪验证用户为合法用户，开始扫描用户请求所要扫描的原始文档，获取到扫描文档。用户在扫描仪上扫描文档时，输入第二验证码，通过身份验证后扫描仪即知道该向哪个本机发送扫描的文档。即使没有 GUI 或数字键的情况下，仅仅通过某些按键的按键顺序等识别不同的用户。

[0089] 步骤 S506，扫描仪根据该本机目录扫描文档至与验证码对应的云端位置。

[0090] 在该实施例中，图 2 中的步骤 S106 和 S108 可以通过步骤 S306 来实现，具体地，扫描仪在验证用户为合法用户之后，扫描用户所要扫描的原始文档，获取到扫描文档，然后，扫描仪根据从 EWS 程序中获取该本机目录即第一验证码与云端位置的关联关系，获取到目标存储地址，直接将扫描文档存储在云端位置中。其中，云端位置还可以是 Email 地址或网络打印机的名称或设定信息。在该实施例中，不需要将扫描文档扫描到主机客户端上的文件夹，再通过主机客户端发送到其他地方，也不需要在扫描仪上记录或输入云端位置、Email 地址或网络打印机的名称或设定信息，扫描仪通过共享服务器创建的第一验证码与存储地址的关联关系，可以直接得到用户设定的存储地址，实现了安全简便进行网络扫描的效果。

[0091] 步骤 S507，结束扫描，关闭共享服务器 EWS。

[0092] 具体地，结束扫描，第一验证码失效，用户可以关闭共享服务器 EWS。用户扫描完成后本机目录共享关系、第一验证码失效，则用户下一次使用该第一验证码进行身份验证的时候不能通过身份验证，从而不能使用扫描功能，进而保证了扫描系统的安全性。

[0093] 需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0094] 图 6 是根据本发明的扫描仪的结构示意图。如图 6 所示，该扫描仪包括：获取装置 10，用于获取主机客户端的扫描请求及由扫描请求所生成的第一验证码；比较器 30，用于在获取到用户输入的第二验证码之后，在第一验证码与第二验证码匹配的情况下，验证用户为合法用户；扫描装置 50，用于在验证用户为合法用户之后，扫描用户请求所要扫描的原始文档，以获取扫描文档；发送装置 70，用于从共享服务器上获取与第一验证码相对应的存储地址，并将获取到的扫描文档发送到存储地址；其中，在获取到由扫描请求所生成的第一验证码之后，将第一验证码发送到共享服务器，以创建第一验证码与存储地址的关联关系。

[0095] 采用本发明的扫描仪，通过获取装置获取到主机客户端发送的扫描请求及由扫描请求所生成的第一验证码，然后比较器在获取到用户输入的第二验证码之后，在第一验证

码与第二验证码匹配的情况下,验证用户为合法用户,之后通过扫描装置扫描用户请求所要扫描的原始文档,在获取到扫描文档之后,发送装置从共享服务器上获取与第一验证码相对应的存储地址,并将获取到的扫描文档发送到存储地址,其中,共享服务器连接于主机客户端与扫描仪之间,可以根据获取到的第一验证码,创建第一验证码与存储地址的关联关系。通过本发明提供的扫描系统,用户通过主机客户端发送扫描请求,在扫描仪端验证为合法用户之后,才可以在扫描仪扫描用户需要扫描的文档,增加了扫描的安全性,并且在扫描仪获取到扫描文档之后,通过共享服务器获取用户设定的存储地址,而不是直接将扫描文档发送到本机,解决了现有技术中利用网络扫描文档的方法具有安全性隐患的问题,进而实现了安全、简便地进行网络扫描的技术效果。

[0096] 从以上的描述中,可以看出,本发明实现了如下技术效果:在本发明的上述实施例中,利用共享服务器 EWS(embedded web server) 等 web 程序访问到扫描仪,向扫描仪发出要扫描到本机的请求,扫描仪发送第一验证码给用户,或 PC 向扫描仪器发送地验证码及请求扫描,用户在扫描仪上扫描文档时,输入验证码,扫描仪从 EWS 上获取用户设定的存储地址并向那个地址发送扫描的文档。即使没有 GUI 或数字键的情况下,仅仅通过某些 button 的按键顺序等,扫描仪也能识别不同的用户,并且该第一验证码在用户操作后或一段时间后失效。通过本发明提供的扫描方法及系统,用户通过主机客户端发送扫描请求之后,用户在扫描仪端通过身份验证并在扫描仪获取到扫描文档之后,扫描仪从共享服务器上获取存储扫描文档的地址,并将扫描文档发送到用户设定的存储地址,然而现有技术中需要将扫描文件存储在本机然后在发送到其他地址,本发明直接将扫描文档存储在用户需要的存储位置,并且验证码的临时验证使得整个扫描过程都很安全,解决了现有技术中利用网络扫描文档的方法具有安全性隐患且操作繁琐的问题,进而实现了安全、简便地进行网络扫描的技术效果。

[0097] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。

[0098] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

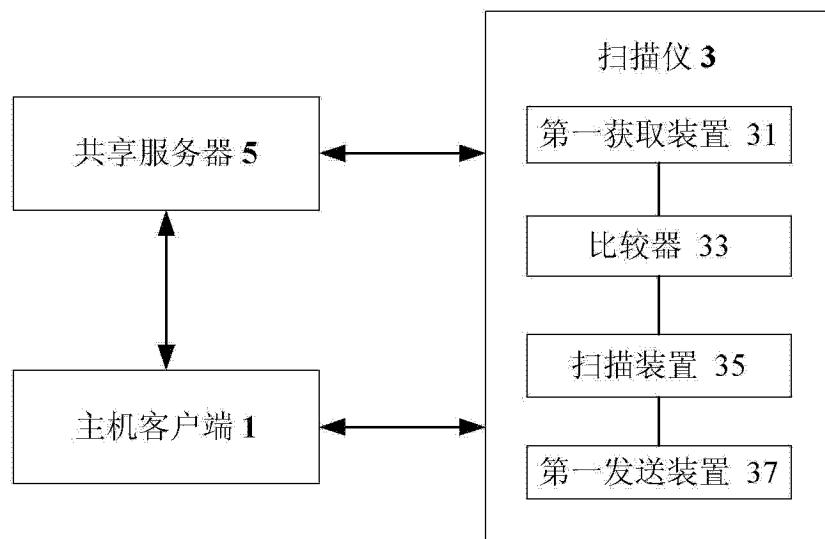


图 1

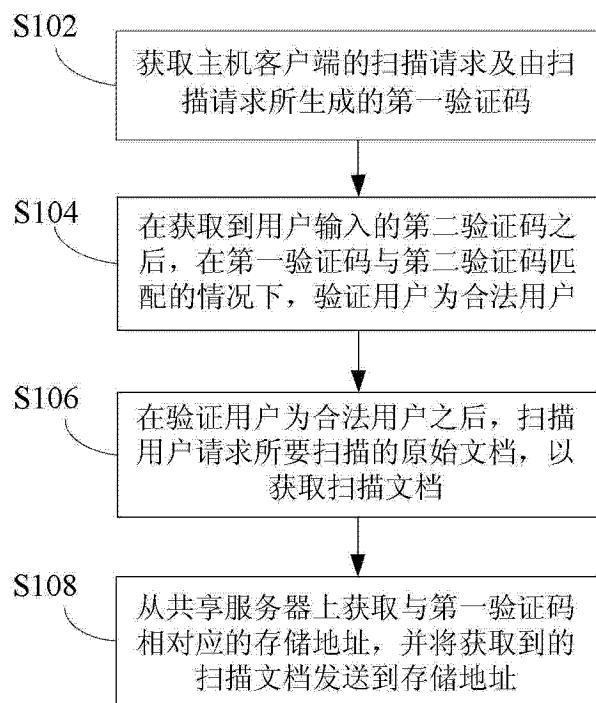


图 2

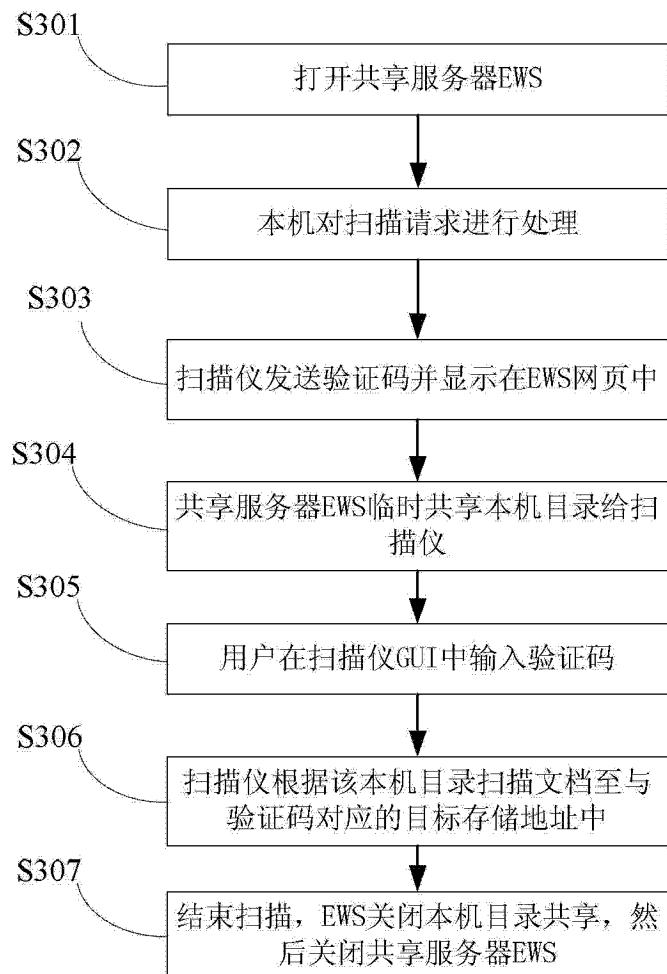


图 3

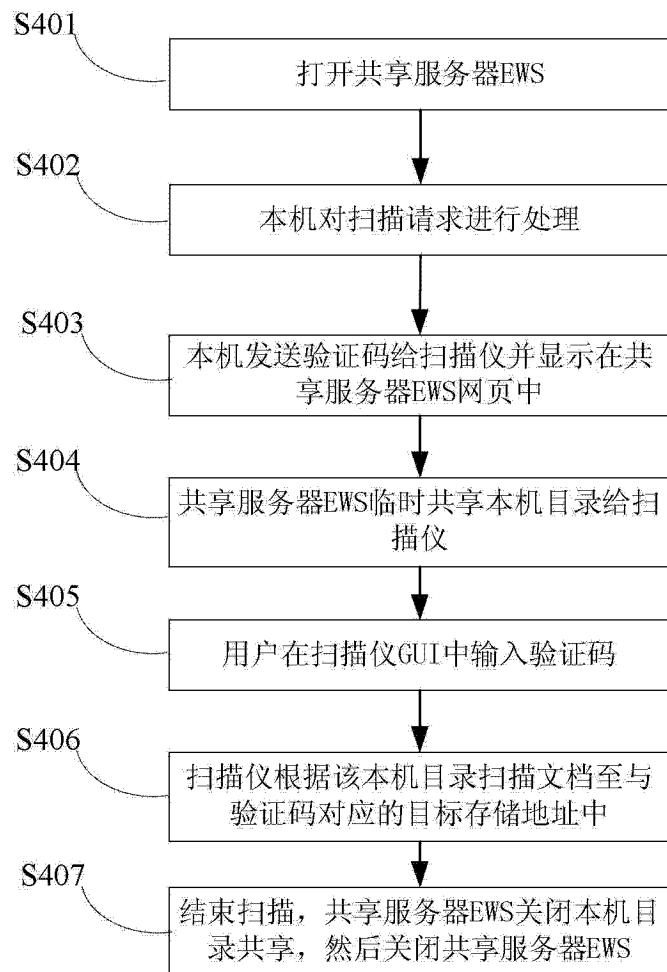


图 4

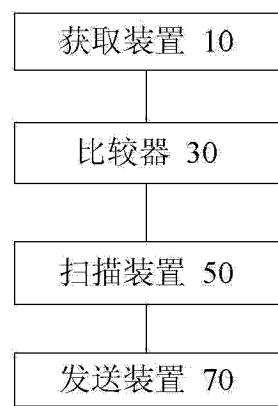
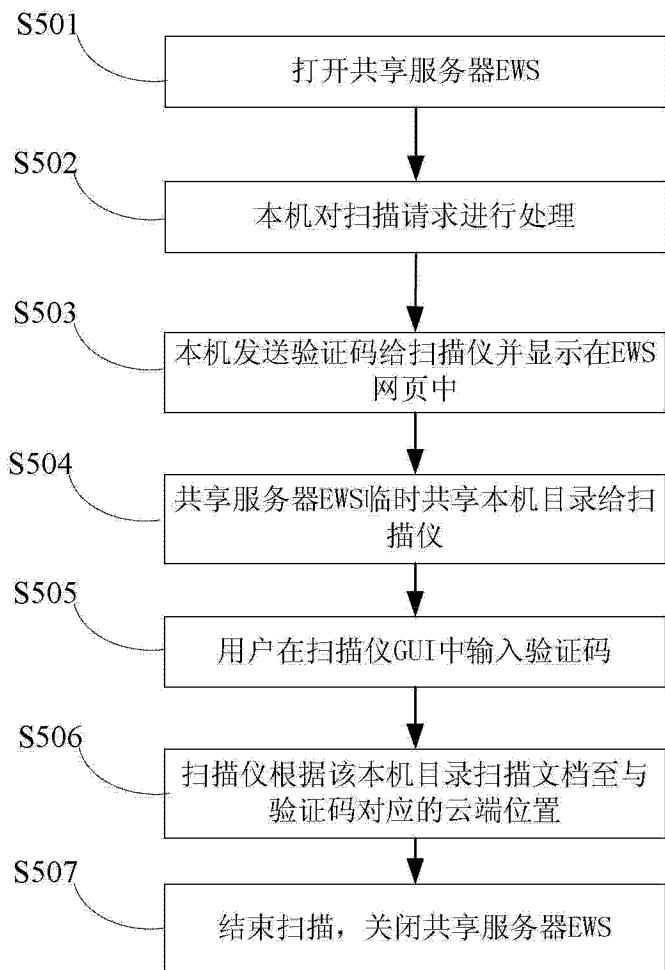


图 6