(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106372473 A
(43)申请公布日 2017.02.01

(21)申请号 201610800749.3

(22)申请日 2016.09.02

(71)申请人 深圳中兴网信科技有限公司
地址 518057 广东省深圳市南山区高新区南区科技南路中兴通讯一期A座(中兴综合大楼厂房)三楼317房

(72)发明人 陈友雄 吴建军

(74)专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343
代理人 尚志峰 汪海屏

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/45(2013.01)
G06F 21/62(2013.01)

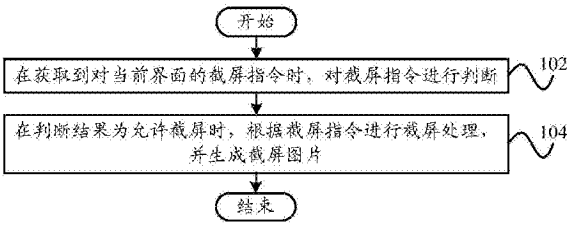
权利要求书3页 说明书14页 附图4页

(54)发明名称

截屏方法、截屏装置、终端和服务器

(57)摘要

本发明提供了一种截屏方法、截屏装置、终端和服务器，其中，截屏方法包括：在获取到对当前界面的截屏指令时，对截屏指令进行判断；在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片。通过本发明技术方案，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。



CN 106372473 A

1.一种截屏方法，适用于终端，其特征在于，包括：

在获取到对当前界面的截屏指令时，对所述截屏指令进行判断；

在所述判断结果为允许截屏时，根据所述截屏指令进行截屏处理，并生成截屏图片。

2.根据权利要求1所述的截屏方法，其特征在于，所述在获取到对当前界面的截屏指令时，对所述截屏指令进行判断，具体包括以下步骤：

确定所述当前界面所属的应用程序；

根据所述应用程序确定对应的截屏状态参数；

根据所述截屏状态参数判断是否允许截屏。

3.根据权利要求2所述的截屏方法，其特征在于，所述在获取到对当前界面的截屏指令时，对所述截屏指令进行判断前，还包括：

预设所述应用程序与所述截屏状态参数的对应关系。

4.根据权利要求3所述的截屏方法，其特征在于，所述根据所述应用程序确定对应的截屏状态参数，具体包括以下步骤：

确定所述应用程序的显示状态属性值；

根据所述对应关系将所述显示状态属性值修改为所述截屏状态参数。

5.根据权利要求3所述的截屏方法，其特征在于，所述在获取到对当前界面的截屏指令时，对所述截屏指令进行判断前，还包括：

检测所述当前界面的显示对象中是否包含预设目标显示对象；

在检测到所述显示对象中包含所述预设目标显示对象时，允许截屏；

在检测扫所述显示对象中不包含所述预设目标显示对象时，不允许截屏。

6.根据权利要求1所述的截屏方法，其特征在于，所述在获取到对当前界面的截屏指令时，对所述截屏指令进行判断，具体还包括以下步骤：

确定用户权限信息；

根据所述用户权限信息判断是否允许截屏。

7.根据权利要求2所述的截屏方法，其特征在于，所述在所述判断结果为允许截屏时，根据所述截屏指令进行截屏处理，并生成截屏图片，具体包括以下步骤：

在所述判断结果为允许截屏时，确定所述应用程序的用户权限信息；

根据所述用户权限信息确定所述截屏指令的执行方式，以根据所述执行方式生成所述截屏图片。

8.根据权利要求7所述的截屏方法，其特征在于，所述根据所述用户权限信息确定所述截屏指令的执行方式，以根据所述执行方式生成所述截屏图片，具体包括以下步骤：

检测所述用户权限信息中是否包括操作权限；

在检测到所述用户权限信息中包括所述操作权限时，执行所述截屏指令。

9.根据权利要求8所述的截屏方法，其特征在于，还包括：

在检测到所述用户权限信息不包括所述操作权限时，确定所述用户权限信息确定对应的截屏信息处理方式；

根据所述截屏信息处理方式生成处理后的截屏图片。

10.根据权利要求9所述的截屏方法，其特征在于，所述根据所述截屏信息处理方式生成处理后的截屏图片，具体包括以下步骤：

确定所述当前界面的敏感信息；

对所述敏感信息执行屏蔽操作，以生成所述处理后的截屏图片。

11.一种截屏装置，适用于终端，其特征在于，包括：

判断单元，用于在获取到对当前界面的截屏指令时，对所述截屏指令进行判断；

截屏处理单元，用于在所述判断结果为允许截屏时，根据所述截屏指令进行截屏处理，并生成截屏图片。

12.根据权利要求11所述的截屏装置，其特征在于，还包括：

确定单元，用于确定所述当前界面所属的应用程序；

所述确定单元还用于：根据所述应用程序确定对应的截屏状态参数；

所述判断单元还用于：根据所述截屏状态参数判断是否允许截屏。

13.根据权利要求12所述的截屏装置，其特征在于，还包括：

预设单元，用于预设所述应用程序与所述截屏状态参数的对应关系。

14.根据权利要求12所述的截屏装置，其特征在于，

所述确定单元还用于：确定所述应用程序的显示状态属性值；

所述截屏装置还包括：

修改单元，用于根据所述对应关系将所述显示状态属性值修改为所述截屏状态参数。

15.根据权利要求13所述的截屏装置，其特征在于，还包括：

检测单元，用于检测所述当前界面的显示对象中是否包含预设目标显示对象；

所述截屏处理单元还用于：在检测到所述显示对象中包含所述预设目标显示对象时，允许截屏；

所述截屏处理单元还用于：在检测扫所述显示对象中不包含所述目标显示对象时，不允许截屏。

16.根据权利要求11所述的截屏装置，其特征在于，

所述确定单元还用于：确定用户权限信息；

所述判断单元还用于：根据所述用户权限信息判断是否允许截屏。

17.根据权利要求12所述的截屏装置，其特征在于，

所述确定单元还用于：在所述判断结果为允许截屏时，确定所述应用程序的用户权限信息；

所述确定单元还用于：根据所述用户权限信息确定所述截屏指令的执行方式，以根据所述执行方式生成所述截屏图片。

18.根据权利要求17所述的截屏装置，其特征在于，

所述检测单元还用于：检测所述用户权限信息中是否包括操作权限；

所述截屏装置还包括：

执行单元，用于在检测到所述用户权限信息中包括所述操作权限时，执行所述截屏指令。

19.根据权利要求18所述的截屏装置，其特征在于，

所述确定单元还用于：在检测到所述用户权限信息不包括所述操作权限时，确定所述用户信息确定对应的截屏信息处理方式；

所述截屏处理单元还用于：根据所述截屏信息处理方式生成处理后的截屏图片。

20.根据权利要求19所述的截屏装置，其特征在于，

所述确定单元还用于：确定所述当前界面的敏感信息；

所述截屏装置还包括：

屏蔽单元，用于对所述敏感信息执行屏蔽操作，以生成所述处理后的截屏图片。

21.一种终端，其特征在于，包括：如权利要求11至20中任一项所述的截屏装置。

22.一种截屏方法，适用于服务器，其特征在于，包括：

在接收到终端发送的应用程序的登陆信息时，根据所述登陆信息确定对应的截屏状态参数；

将所述截屏状态参数发送至所述终端，以使所述终端根据所述截屏状态参数对截屏指令进行判断，以确定是否根据所述截屏指令进行截屏处理。

23.根据权利要求22所述的截屏方法，其特征在于，还包括：

在接收到所述终端发送的所述应用程序的用户信息时，根据所述用户信息确定对应的截屏策略；

将所述截屏策略发送至所述终端，以使所述终端根据所述截屏策略确定所述截屏指令的执行方式。

24.根据权利要求22所述的截屏方法，其特征在于，所述在接收到终端发送的应用程序的登陆信息时，根据所述登陆信息确定对应的截屏状态参数前，还包括：

预存所述应用程序对应的所述截屏状态参数。

25.一种截屏装置，适用于服务器，其特征在于，包括：

确定单元，用于在接收到终端发送的应用程序的登陆信息时，根据所述登陆信息确定对应的截屏状态参数；

发送单元，用于将所述截屏状态参数发送至所述终端，以使所述终端根据所述截屏状态参数对截屏指令进行判断，以确定是否根据所述截屏指令进行截屏处理。

26.根据权利要求25所述的截屏装置，其特征在于，

所述确定单元还用于：在接收到所述终端发送的所述应用程序的用户信息时，根据所述用户信息确定对应的截屏策略；

所述发送单元还用于：将所述截屏策略发送至所述终端，以使所述终端根据所述截屏策略确定所述截屏指令的执行方式。

27.根据权利要求25所述的截屏装置，其特征在于，还包括：

预存单元，用于预存所述应用程序对应的所述截屏状态参数。

28.一种服务器，其特征在于，包括：如权利要求25至27中任一项所述的截屏装置。

截屏方法、截屏装置、终端和服务器

技术领域

[0001] 本发明涉及终端技术领域，具体而言，涉及一种截屏方法、一种截屏装置、一种终端和一种服务器。

背景技术

[0002] 在相关技术中，为了提高办公的便捷性并实现移动办公，部分公司使用手机等移动终端代替个人计算机进行办公，但是在使用移动终端办公时，由于存在移动网络的安全性、终端信息存储的安全性以及数据传输的安全性等安全问题，易造成信息泄露，例如手机上的某些涉密信息通过截屏的方式被拷贝并进行传播，从而给公司与个人造成不可预计的损失。

[0003] 因此，如何设计一种新的截屏方案，以提高截屏控制的安全性成为亟待解决的技术问题。

发明内容

[0004] 本发明正是基于上述技术问题至少之一，提出了一种新的截屏方案，通过在获取到对当前界面的截屏指令时，对截屏指令进行判断，以确定是否允许截屏，在判断结果为允许截屏时，则根据截屏指令生成截屏图片，在判断结果为不允许截屏时，则不执行截屏操作，通过对截屏指令进行判断，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。

[0005] 有鉴于此，本发明提出了一种截屏方法，包括：在获取到对当前界面的截屏指令时，对截屏指令进行判断；在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片。

[0006] 在该技术方案中，通过在获取到对当前界面的截屏指令时，对截屏指令进行判断，以确定是否允许截屏，在判断结果为允许截屏时，则根据截屏指令生成截屏图片，在判断结果为不允许截屏时，则不执行截屏操作，通过对截屏指令进行判断，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。

[0007] 具体地，可以预设一个应用程序的截屏管理策略，截屏管理策略包括截屏状态参数和登陆应用程序的用户信息，比如根据截屏状态参数确定是否执行截屏指令，或根据用户的操作权限确定是否执行截屏指令。

[0008] 在上述技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断，具体包括以下步骤：确定当前界面所属的应用程序；根据应用程序确定对应的截屏状态参数；根据截屏状态参数判断是否允许截屏。

[0009] 在该技术方案中，通过当前界面确定所属的应用程序，并根据应用程序确定对应的截屏状态参数，以根据截屏状态参数确定是否允许截屏，实现了针对不同应用程序确定不同的截屏状态，以确定是否进行截屏。

[0010] 其中，截屏状态包括允许直接截屏操作、不允许截屏操作，允许对指令界面进行截

屏操作，允许根据特定方式处理后执行截屏操作等。

[0011] 在上述任一项技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断前，还包括：预设应用程序与截屏状态参数的对应关系。

[0012] 在该技术方案中，通过预设应用程序与截屏状态参数的对应关系，在获取到截屏指令时，能够通过应用程序确定对应的截屏状态参数，以确定是否执行对应用程序的界面的截屏指令，实现了对指定的应用程序不允许截屏或有条件的允许截屏，提升了用户在应用程序使用过程中的安全性，防止了应用程序涉及到的机密信息被泄露。

[0013] 具体地，对于保密性强的应用程序，比如涉及公司营运报表的应用程序，只允许进行查看，则可以将对应的截屏状态参数设置为不可截屏。

[0014] 另外，通过预设应用程序与截屏状态参数的对应关系，实现了不是在系统运行时就进行信息安全控制，而是在用户进行不安全操作的时候才进行安全控制，不但让系统负担更轻，同时也让用户感觉不到角色壁垒和歧视。

[0015] 在上述任一项技术方案中，优选地，根据应用程序确定对应的截屏状态参数，具体包括以下步骤：确定应用程序的显示状态属性值；根据对应关系将显示状态属性值修改为截屏状态参数。

[0016] 在该技术方案中，通过修改应用程序的显示状态属性值，确定应用程序的截屏状态参数，以确定是否执行截屏操作。

[0017] 具体地，以android系统为例，可以通过SDK(Software Development Kit，软件开发工具包)将surface.java的状态属性值true和false修改为其它参数，以生成不同的截屏状态参数。

[0018] 在上述任一项技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断前，还包括：检测当前界面的显示对象中是否包含预设目标显示对象；在检测到显示对象中包含预设目标显示对象时，允许截屏；在检测扫显示对象中不包含预设目标显示对象时，不允许截屏。

[0019] 在该技术方案中，通过预设显示对象确定规则，以根据显示对象确定规则，从当前界面包含的显示对象中确定目标显示对象，当不存在目标显示对象时，则不允许截屏，从而根据显示对象确定规则确定截屏状态参数。

[0020] 在上述任一项技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断，具体还包括以下步骤：确定用户权限信息；根据用户权限信息判断是否允许截屏。

[0021] 在该技术方案中，通过确定用户权限信息，并根据用户权限信息判断是否允许截屏，能够针对不同的用户确定不同的截屏权限，满足了不同用户的使用需求，其中，用户权限信息中的用户可以是操作系统登陆时对应的用户，也可以是登陆指定的应用程序时对应的用户。

[0022] 具体地，不同的用户具备不同的操作权限，比如普通员工只具备查看权限，无法进行截屏操作，中层管理人员只对指定的应用程序具有截屏权限，而高层原理人员具备对所有应用程序的截屏权限，通过用户权限信息判断是否允许截屏，提升了截屏的安全性。

[0023] 在上述任一项技术方案中，优选地，在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片，具体包括以下步骤：在判断结果为允许截屏时，确定应用程序

的用户权限信息;根据用户权限信息确定截屏指令的执行方式,以根据执行方式生成截屏图片。

[0024] 在该技术方案中,通过在判断结果为允许截屏时,确定应用程序的用户权限信息,以根据用户的权限信息确定是直接对当前界面进行截屏,还是在进行处理后截屏,通过对不同的用户进行不同的权限划分,使不同用户针对不同功能得到不同的截屏效果,使截屏操作更加人性化。

[0025] 其中,应用程序的用户权限信息可以与用户登录应用程序的登陆信息对应。

[0026] 在上述任一项技术方案中,优选地,根据用户权限信息确定截屏指令的执行方式,以根据执行方式生成截屏图片,具体包括以下步骤:检测用户权限信息中是否包括操作权限;在检测到用户权限信息中包括操作权限时,执行截屏指令。

[0027] 在该技术方案中,在检测到用户权限信息中包括操作权限时,直接执行截屏指令,具备操作权限的用户可以直接进行截屏操作,满足了用户截屏操作需求。

[0028] 在上述任一项技术方案中,优选地,还包括:在检测到用户权限信息不包括操作权限时,确定用户权限信息确定对应的截屏信息处理方式;根据截屏信息处理方式生成处理后的截屏图片。

[0029] 在该技术方案中,在检测到用户权限信息不包括操作权限时,即用户不能够直接执行截屏操作,此时确定用户权限信息对应的截屏处理方式,以根据截屏处理方式生成处理后的截屏图片,通过对用户的权限划分,确定对应的截屏处理方式,实现了在截屏时多样化的处理,使不同用户对同一界面进行截屏也具备差异性,同时满足了不同环境中对截屏图片处理的需求。

[0030] 当应用程序获得截屏授权指令时,根据当前用户的权限信息给出当前界面的截屏界面。

[0031] 其中,截屏处理方式包括对待生成的截屏图片进行雾化处理,在底层添加包括公司LOGO的水印,屏蔽界面上的关键信息,以及生成白屏图片等。

[0032] 在上述任一项技术方案中,优选地,根据截屏信息处理方式生成处理后的截屏图片,具体包括以下步骤:确定当前界面的敏感信息;对敏感信息执行屏蔽操作,以生成处理后的截屏图片。

[0033] 在该技术方案中,通过确定当前界面的敏感信息,并对敏感信息执行屏蔽操作,以生成处理后的截屏图片,防止了敏感信息的外泄,提升了截屏操作的安全性,并且细化了截屏效果。

[0034] 敏感信息包括公司的机密信息、用户的个人资料等。

[0035] 根据本发明第二方面,还提出了一种截屏装置,包括:判断单元,用于在获取到对当前界面的截屏指令时,对截屏指令进行判断;截屏处理单元,用于在判断结果为允许截屏时,根据截屏指令进行截屏处理,并生成截屏图片。

[0036] 在该技术方案中,通过在获取到对当前界面的截屏指令时,对截屏指令进行判断,以确定是否允许截屏,在判断结果为允许截屏时,则根据截屏指令生成截屏图片,在判断结果为不允许截屏时,则不执行截屏操作,通过对截屏指令进行判断,防止了具有敏感信息与保密信息的页面被截屏传播,提高了截屏操作的安全性,提升了用户的使用体验。

[0037] 具体地,可以预设一个应用程序的截屏管理策略,截屏管理策略包括截屏状态参

数和登陆应用程序的用户信息，比如根据截屏状态参数确定是否执行截屏指令，或根据用户的操作权限确定是否执行截屏指令。

[0038] 在上述技术方案中，优选地，还包括：确定单元，用于确定当前界面所属的应用程序；确定单元还用于：根据应用程序确定对应的截屏状态参数；判断单元还用于：根据截屏状态参数判断是否允许截屏。

[0039] 在该技术方案中，通过当前界面确定所属的应用程序，并根据应用程序确定对应的截屏状态参数，以根据截屏状态参数确定是否允许截屏，实现了针对不同应用程序确定不同的截屏状态，以确定是否进行截屏。

[0040] 其中，截屏状态包括允许直接截屏操作、不允许截屏操作，允许对指令界面进行截屏操作，允许根据特定方式处理后执行截屏操作等。

[0041] 具体地，可以通过修改状态属性确定截屏状态，比如在android系统中，可以通过SDK(Software Development Kit，软件开发工具包)将surface.java的状态属性值true和false修改为其它参数，以生成不同的截屏状态参数。

[0042] 另外，也可以通过预设显示对象的确定规则确定截屏状态，以根据显示对象的确定规则，检测当前界面包含的显示对象中是否存在目标显示对象，当存在目标显示对象时，允许截屏，当不存在目标显示对象时，则不允许截屏，从而根据显示对象确定规则确定截屏状态参数。

[0043] 在上述任一项技术方案中，优选地，还包括：预设单元，用于预设应用程序与截屏状态参数的对应关系。

[0044] 在该技术方案中，通过预设应用程序与截屏状态参数的对应关系，在获取到截屏指令时，能够通过应用程序确定对应的截屏状态参数，以确定是否执行对应用程序的界面的截屏指令，实现了对指定的应用程序不允许截屏或有条件的允许截屏，提升了用户在应用程序使用过程中的安全性，防止了应用程序涉及到的机密信息被泄露。

[0045] 具体地，对于保密性强的应用程序，比如涉及公司营运报表的应用程序，只允许进行查看，则可以将对应的截屏状态参数设置为不可截屏。

[0046] 另外，通过预设应用程序与截屏状态参数的对应关系，实现了不是在系统运行时就进行信息安全控制，而是在用户进行不安全操作的时候才进行安全控制，不但让系统负担更轻，同时也让用户感觉不到角色壁垒和歧视。

[0047] 在上述任一项技术方案中，优选地，确定单元还用于：确定应用程序的显示状态属性值；截屏装置还包括：修改单元，用于根据对应关系将显示状态属性值修改为截屏状态参数。

[0048] 在该技术方案中，通过修改应用程序的显示状态属性值，确定应用程序的截屏状态参数，以确定是否执行截屏操作。

[0049] 具体地，以android系统为例，可以通过SDK(Software Development Kit，软件开发工具包)将surface.java的状态属性值true和false修改为其它参数，以生成不同的截屏状态参数。

[0050] 在上述任一项技术方案中，优选地，还包括：检测单元，用于检测当前界面的显示对象中是否包含预设目标显示对象；截屏处理单元还用于：在检测到显示对象中包含预设目标显示对象时，允许截屏；截屏处理单元还用于：在检测扫显示对象中不包含目标显示对

象时，不允许截屏。

[0051] 在上述任一项技术方案中，优选地，确定单元还用于：确定用户权限信息；判断单元还用于：根据用户权限信息判断是否允许截屏。

[0052] 在该技术方案中，通过确定用户权限信息，并根据用户权限信息判断是否允许截屏，能够针对不同的用户确定不同的截屏权限，满足了不同用户的使用需求，其中，用户权限信息中的用户可以是操作系统登陆时对应的用户，也可以是登陆指定的应用程序时对应的用户。

[0053] 具体地，不同的用户具备不同的操作权限，比如普通员工只具备查看权限，无法进行截屏操作，中层管理人员只对指定的应用程序具有截屏权限，而高层原理人员具备对所有应用程序的截屏权限，通过用户权限信息判断是否允许截屏，提升了截屏的安全性。

[0054] 在上述任一项技术方案中，优选地，确定单元还用于：在判断结果为允许截屏时，确定应用程序的用户权限信息；确定单元还用于：根据用户权限信息确定截屏指令的执行方式，以根据执行方式生成截屏图片。

[0055] 在该技术方案中，通过在判断结果为允许截屏时，确定应用程序的用户权限信息，以根据用户的权限信息确定是直接对当前界面进行截屏，还是在进行处理后截屏，通过对不同的用户进行不同的权限划分，使不同用户针对不同功能得到不同的截屏效果，使截屏操作更加人性化。

[0056] 其中，应用程序的用户权限信息可以与用户登录应用程序的登陆信息对应。

[0057] 在上述任一项技术方案中，优选地，检测单元还用于：检测用户权限信息中是否包括操作权限；截屏装置还包括：执行单元，用于在检测到用户权限信息中包括操作权限时，执行截屏指令。

[0058] 在该技术方案中，在检测到用户权限信息中包括操作权限时，直接执行截屏指令，具备操作权限的用户可以直接进行截屏操作，满足了用户截屏操作需求。

[0059] 在上述任一项技术方案中，优选地，确定单元还用于：在检测到用户权限信息不包括操作权限时，确定用户信息确定对应的截屏信息处理方式；截屏处理单元还用于：根据截屏信息处理方式生成处理后的截屏图片。

[0060] 在该技术方案中，在检测到用户权限信息不包括操作权限时，即用户不能够直接执行截屏操作，此时确定用户权限信息对应的截屏处理方式，以根据截屏处理方式生成处理后的截屏图片，通过对用户的权限划分，确定对应的截屏处理方式，实现了在截屏时多样化的处理，使不同用户对同一界面进行截屏也具备差异性，同时满足了不同环境中对截屏图片处理的需求。

[0061] 当应用程序获得截屏授权指令时，根据当前用户的权限信息给出当前界面的截屏界面。

[0062] 其中，截屏处理方式包括对待生成的截屏图片进行雾化处理，在底层添加包括公司LOGO的水印，屏蔽界面上的关键信息，以及生成白屏图片等。

[0063] 在上述任一项技术方案中，优选地，确定单元还用于：确定当前界面的敏感信息；截屏装置还包括：屏蔽单元，用于对敏感信息执行屏蔽操作，以生成处理后的截屏图片。

[0064] 在该技术方案中，通过确定当前界面的敏感信息，并对敏感信息执行屏蔽操作，以生成处理后的截屏图片，防止了敏感信息的外泄，提升了截屏操作的安全性，并且细化了截

屏效果。

[0065] 敏感信息包括公司的机密信息、用户的个人资料等。

[0066] 根据本发明第三方面，还提出了一种终端，包括上述任一项技术方案所述的截屏装置，因此，该终端包括上述任一项技术方案所述的截屏装置的技术效果，在此不再赘述。

[0067] 根据本发明第四方面，还提出了一种截屏方法，包括：在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数；将截屏状态参数发送至终端，以使终端根据截屏状态参数对截屏指令进行判断，以确定是否根据截屏指令进行截屏处理。

[0068] 在该技术方案中，服务器在接收到终端的登陆信息时，根据登陆信息确定对应的截屏状态参数，并将截屏状态参数发送至终端，以使终端在获取到截屏指令时，根据截屏状态参数对截屏指令进行判断，来确定是否进行截屏处理，通过应用程序与截屏状态参数的对应关系，在实现了服务器与终端交互的同时，根据不同的应用程序确定不同的截屏状态，实现了截屏指令处理的多样化，满足了用户对截屏不同处理方式的需求。

[0069] 其中，服务器具体为管理服务器，可以是应用程序服务器，也可以是其它局域网服务器。

[0070] 在上述技术方案中，优选地，还包括：在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略；将截屏策略发送至终端，以使终端根据截屏策略确定截屏指令的执行方式。

[0071] 在该技术方案中，服务器在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略，并将截屏策略发送至终端，以使终端根据截屏策略进行具体的截屏操作，从而体现了用户截屏操作的差异化，满足了不同用户使用的需求。

[0072] 在上述任一项技术方案中，优选地，在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数前，还包括：预存应用程序对应的截屏状态参数。

[0073] 在该技术方案中，通过在服务器中预存对应的截屏状态参数，在终端访问服务器时就能够获得应用程序对应的截屏状态参数，减少了终端本地预设步骤，实现了区域化终端截屏管理，满足了办公的需求。

[0074] 根据本发明第五方面，还提出了一种截屏装置，包括：确定单元，用于在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数；发送单元，用于将截屏状态参数发送至终端，以使终端根据截屏状态参数对截屏指令进行判断，以确定是否根据截屏指令进行截屏处理。

[0075] 在该技术方案中，服务器在接收到终端的登陆信息时，根据登陆信息确定对应的截屏状态参数，并将截屏状态参数发送至终端，以使终端在获取到截屏指令时，根据截屏状态参数对截屏指令进行判断，来确定是否进行截屏处理，通过应用程序与截屏状态参数的对应关系，在实现了服务器与终端交互的同时，根据不同的应用程序确定不同的截屏状态，实现了截屏指令处理的多样化，满足了用户对截屏不同处理方式的需求。

[0076] 在上述技术方案中，优选地，确定单元还用于：在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略；发送单元还用于：将截屏策略发送至终端，以使终端根据截屏策略确定截屏指令的执行方式。

[0077] 在该技术方案中，服务器在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略，并将截屏策略发送至终端，以使终端根据截屏策略进行具体的

截屏操作，从而体现了用户截屏操作的差异化，满足了不同用户使用的需求。

[0078] 在上述任一项技术方案中，优选地，还包括：预存单元，用于预存应用程序对应的截屏状态参数。

[0079] 在该技术方案中，通过在服务器中预存对应的截屏状态参数，在终端访问服务器时就能够获得应用程序对应的截屏状态参数，减少了终端本地预设步骤，实现了区域化终端截屏管理，满足了办公的需求。

[0080] 根据本发明第六方面，还提出了一种服务器，包括上述任一项技术方案所述的截屏装置，因此，该终端包括上述任一项技术方案所述的截屏装置的技术效果，在此不再赘述。

[0081] 通过以上技术方案，通过在获取到对当前界面的截屏指令时，对截屏指令进行判断，以确定是否允许截屏，在判断结果为允许截屏时，则根据截屏指令生成截屏图片，在判断结果为不允许截屏时，则不执行截屏操作，通过对截屏指令进行判断，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。

附图说明

[0082] 图1示出了根据本发明的一个实施例的截屏方法的示意流程图；

[0083] 图2示出了根据本发明的一个实施例的截屏装置的示意框图；

[0084] 图3示出了根据本发明的实施例的终端的示意框图；

[0085] 图4示出了根据本发明的另一个实施例的截屏方法的示意流程图；

[0086] 图5示出了根据本发明的另一个实施例的截屏装置的示意框图；

[0087] 图6示出了根据本发明的实施例的服务器的示意框图；

[0088] 图7示出了根据本发明的一个实施例的截屏方案的示意流程图；

[0089] 图8示出了根据本发明的另一个实施例的截屏方案的示意流程图；

[0090] 图9示出了根据本发明的再一个实施例的截屏方案的示意流程图；

[0091] 图10示出了根据本发明的又一个实施例的截屏方案的示意图；

[0092] 图11与图12示出了根据本发明的又一个实施例的截屏方案的示意图。

具体实施方式

[0093] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[0094] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用第三方不同于在此描述的第三方方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[0095] 图1示出了根据本发明的一个实施例的截屏方法的示意流程图。

[0096] 如图1所示，根据本发明的一个实施例的截屏方法，包括：步骤102，在获取到对当前界面的截屏指令时，对截屏指令进行判断；步骤104，在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片。

[0097] 在该技术方案中，通过在获取到对当前界面的截屏指令时，对截屏指令进行判断，

以确定是否允许截屏，在判断结果为允许截屏时，则根据截屏指令生成截屏图片，在判断结果为不允许截屏时，则不执行截屏操作，通过对截屏指令进行判断，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。

[0098] 具体地，可以预设一个应用程序的截屏管理策略，截屏管理策略包括截屏状态参数和登陆应用程序的用户信息，比如根据截屏状态参数确定是否执行截屏指令，或根据用户的操作权限确定是否执行截屏指令。

[0099] 在上述技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断，具体包括以下步骤：确定当前界面所属的应用程序；根据应用程序确定对应的截屏状态参数；根据截屏状态参数判断是否允许截屏。

[0100] 在该技术方案中，通过当前界面确定所属的应用程序，并根据应用程序确定对应的截屏状态参数，以根据截屏状态参数确定是否允许截屏，实现了针对不同应用程序确定不同的截屏状态，以确定是否进行截屏。

[0101] 其中，截屏状态包括允许直接截屏操作、不允许截屏操作，允许对指令界面进行截屏操作，允许根据特定方式处理后执行截屏操作等。

[0102] 在上述任一项技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断前，还包括：预设应用程序与截屏状态参数的对应关系。

[0103] 在该技术方案中，通过预设应用程序与截屏状态参数的对应关系，在获取到截屏指令时，能够通过应用程序确定对应的截屏状态参数，以确定是否执行对应用程序的界面的截屏指令，实现了对指定的应用程序不允许截屏或有条件的允许截屏，提升了用户在应用程序使用过程中的安全性，防止了应用程序涉及到的机密信息被泄露。

[0104] 具体地，对于保密性强的应用程序，比如涉及公司营运报表的应用程序，只允许进行查看，则可以将对应的截屏状态参数设置为不可截屏。

[0105] 另外，通过预设应用程序与截屏状态参数的对应关系，实现了不是在系统运行时就进行信息安全控制，而是在用户进行不安全操作的时候才进行安全控制，不但让系统负担更轻，同时也让用户感觉不到角色壁垒和歧视。

[0106] 在上述任一项技术方案中，优选地，根据应用程序确定对应的截屏状态参数，具体包括以下步骤：确定应用程序的显示状态属性值；根据对应关系将显示状态属性值修改为截屏状态参数。

[0107] 在该技术方案中，通过修改应用程序的显示状态属性值，确定应用程序的截屏状态参数，以确定是否执行截屏操作。

[0108] 具体地，以android系统为例，可以通过SDK(Software Development Kit，软件开发工具包)将surface.java的状态属性值true和false修改为其它参数，以生成不同的截屏状态参数。

[0109] 在上述任一项技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断前，还包括：检测当前界面的显示对象中是否包含预设目标显示对象；在检测到显示对象中包含预设目标显示对象时，允许截屏；在检测扫显示对象中不包含预设目标显示对象时，不允许截屏。

[0110] 在该技术方案中，通过预设显示对象确定规则，以根据显示对象确定规则，从当前界面包含的显示对象中确定目标显示对象，当不存在目标显示对象时，则不允许截屏，从而

根据显示对象确定规则确定截屏状态参数。

[0111] 在上述任一项技术方案中，优选地，在获取到对当前界面的截屏指令时，对截屏指令进行判断，具体还包括以下步骤：确定用户权限信息；根据用户权限信息判断是否允许截屏。

[0112] 在该技术方案中，通过确定用户权限信息，并根据用户权限信息判断是否允许截屏，能够针对不同的用户确定不同的截屏权限，满足了不同用户的使用需求，其中，用户权限信息中的用户可以是操作系统登陆时对应的用户，也可以是登陆指定的应用程序时对应的用户。

[0113] 具体地，不同的用户具备不同的操作权限，比如普通员工只具备查看权限，无法进行截屏操作，中层管理人员只对指定的应用程序具有截屏权限，而高层原理人员具备对所有应用程序的截屏权限，通过用户权限信息判断是否允许截屏，提升了截屏的安全性。

[0114] 在上述任一项技术方案中，优选地，在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片，具体包括以下步骤：在判断结果为允许截屏时，确定应用程序的用户权限信息；根据用户权限信息确定截屏指令的执行方式，以根据执行方式生成截屏图片。

[0115] 在该技术方案中，通过在判断结果为允许截屏时，确定应用程序的用户权限信息，以根据用户的权限信息确定是直接对当前界面进行截屏，还是在进行处理后截屏，通过对不同的用户进行不同的权限划分，使不同用户针对不同功能得到不同的截屏效果，使截屏操作更加人性化。

[0116] 其中，应用程序的用户权限信息可以与用户登录应用程序的登陆信息对应。

[0117] 在上述任一项技术方案中，优选地，根据用户权限信息确定截屏指令的执行方式，以根据执行方式生成截屏图片，具体包括以下步骤：检测用户权限信息中是否包括操作权限；在检测到用户权限信息中包括操作权限时，执行截屏指令。

[0118] 在该技术方案中，在检测到用户权限信息中包括操作权限时，直接执行截屏指令，具备操作权限的用户可以直接进行截屏操作，满足了用户截屏操作需求。

[0119] 在上述任一项技术方案中，优选地，还包括：在检测到用户权限信息不包括操作权限时，确定用户权限信息确定对应的截屏信息处理方式；根据截屏信息处理方式生成处理后的截屏图片。

[0120] 在该技术方案中，在检测到用户权限信息不包括操作权限时，即用户不能够直接执行截屏操作，此时确定用户权限信息对应的截屏处理方式，以根据截屏处理方式生成处理后的截屏图片，通过对用户的权限划分，确定对应的截屏处理方式，实现了在截屏时多样化的处理，使不同用户对同一界面进行截屏也具备差异性，同时满足了不同环境中对截屏图片处理的需求。

[0121] 当应用程序获得截屏授权指令时，根据当前用户的权限信息给出当前界面的截屏界面。

[0122] 其中，截屏处理方式包括对待生成的截屏图片进行雾化处理，在底层添加包括公司LOGO的水印，屏蔽界面上的关键信息，以及生成白屏图片等。

[0123] 在上述任一项技术方案中，优选地，根据截屏信息处理方式生成处理后的截屏图片，具体包括以下步骤：确定当前界面的敏感信息；对敏感信息执行屏蔽操作，以生成处理

后的截屏图片。

[0124] 在该技术方案中，通过确定当前界面的敏感信息，并对敏感信息执行屏蔽操作，以生成处理后的截屏图片，防止了敏感信息的外泄，提升了截屏操作的安全性，并且细化了截屏效果。

[0125] 其中，敏感信息包括公司的机密信息、用户的个人资料等。

[0126] 图2示出了根据本发明的一个实施例的截屏装置的示意框图

[0127] 如图2所示，根据本发明的一个实施例的截屏装置200，包括：判断单元202，用于在获取到对当前界面的截屏指令时，对截屏指令进行判断；截屏处理单元204，用于在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片。

[0128] 在该技术方案中，通过在获取到对当前界面的截屏指令时，对截屏指令进行判断，以确定是否允许截屏，在判断结果为允许截屏时，则根据截屏指令生成截屏图片，在判断结果为不允许截屏时，则不执行截屏操作，通过对截屏指令进行判断，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。

[0129] 具体地，可以预设一个应用程序的截屏管理策略，截屏管理策略包括截屏状态参数和登陆应用程序的用户信息，比如根据截屏状态参数确定是否执行截屏指令，或根据用户的操作权限确定是否执行截屏指令。

[0130] 在上述技术方案中，优选地，还包括：确定单元206，用于确定当前界面所属的应用程序；确定单元206还用于：根据应用程序确定对应的截屏状态参数；判断单元202还用于：根据截屏状态参数判断是否允许截屏。

[0131] 在该技术方案中，通过当前界面确定所属的应用程序，并根据应用程序确定对应的截屏状态参数，以根据截屏状态参数确定是否允许截屏，实现了针对不同应用程序确定不同的截屏状态，以确定是否进行截屏。

[0132] 其中，截屏状态包括允许直接截屏操作、不允许截屏操作，允许对指令界面进行截屏操作，允许根据特定方式处理后执行截屏操作等。

[0133] 在上述任一项技术方案中，优选地，还包括：预设单元208，用于预设应用程序与截屏状态参数的对应关系。

[0134] 在该技术方案中，通过预设应用程序与截屏状态参数的对应关系，在获取到截屏指令时，能够通过应用程序确定对应的截屏状态参数，以确定是否执行对应用程序的界面的截屏指令，实现了对指定的应用程序不允许截屏或有条件的允许截屏，提升了用户在应用程序使用过程中的安全性，防止了应用程序涉及到的机密信息被泄露。

[0135] 具体地，对于保密性强的应用程序，比如涉及公司营运报表的应用程序，只允许进行查看，则可以将对应的截屏状态参数设置为不可截屏。

[0136] 另外，通过预设应用程序与截屏状态参数的对应关系，实现了不是在系统运行时就进行信息安全控制，而是在用户进行不安全操作的时候才进行安全控制，不但让系统负担更轻，同时也让用户感觉不到角色壁垒和歧视。

[0137] 在上述任一项技术方案中，优选地，确定单元206还用于：确定应用程序的显示状态属性值；截屏装置200还包括：修改单元210，用于根据对应关系将显示状态属性值修改为截屏状态参数。

[0138] 在该技术方案中，通过修改应用程序的显示状态属性值，确定应用程序的截屏状

态参数，以确定是否执行截屏操作。

[0139] 具体地，以android系统为例，可以通过SDK(Software Development Kit，软件开发工具包)将surface.java的状态属性值true和false修改为其它参数，以生成不同的截屏状态参数。

[0140] 在上述任一项技术方案中，优选地，还包括：检测单元212，用于检测当前界面的显示对象中是否包含预设目标显示对象；截屏处理单元204还用于：在检测到显示对象中包含预设目标显示对象时，允许截屏；截屏处理单元204还用于：在检测扫显示对象中不包含目标显示对象时，不允许截屏。

[0141] 在上述任一项技术方案中，优选地，确定单元206还用于：确定用户权限信息；判断单元202还用于：根据用户权限信息判断是否允许截屏。

[0142] 在该技术方案中，通过确定用户权限信息，并根据用户权限信息判断是否允许截屏，能够针对不同的用户确定不同的截屏权限，满足了不同用户的使用需求，其中，用户权限信息中的用户可以是操作系统登陆时对应的用户，也可以是登陆指定的应用程序时对应的用户。

[0143] 具体地，不同的用户具备不同的操作权限，比如普通员工只具备查看权限，无法进行截屏操作，中层管理人员只对指定的应用程序具有截屏权限，而高层原理人员具备对所有应用程序的截屏权限，通过用户权限信息判断是否允许截屏，提升了截屏的安全性。

[0144] 在上述任一项技术方案中，优选地，确定单元206还用于：在判断结果为允许截屏时，确定应用程序的用户权限信息；确定单元206还用于：根据用户权限信息确定截屏指令的执行方式，以根据执行方式生成截屏图片。

[0145] 在该技术方案中，通过在判断结果为允许截屏时，确定应用程序的用户权限信息，以根据用户的权限信息确定是直接对当前界面进行截屏，还是在进行处理后截屏，通过对不同的用户进行不同的权限划分，使不同用户针对不同功能得到不同的截屏效果，使截屏操作更加人性化。

[0146] 其中，应用程序的用户权限信息可以与用户登录应用程序的登陆信息对应。

[0147] 在上述任一项技术方案中，优选地，检测单元212还用于检测用户权限信息中是否包括操作权限；截屏装置200还包括：执行单元214，用于在检测到用户权限信息中包括操作权限时，执行截屏指令。

[0148] 在该技术方案中，在检测到用户权限信息中包括操作权限时，直接执行截屏指令，具备操作权限的用户可以直接进行截屏操作，满足了用户截屏操作需求。

[0149] 在上述任一项技术方案中，优选地，确定单元206还用于：在检测到用户权限信息不包括操作权限时，确定用户信息确定对应的截屏信息处理方式；截屏处理单元204还用于：根据截屏信息处理方式生成处理后的截屏图片。

[0150] 在该技术方案中，在检测到用户权限信息不包括操作权限时，即用户不能够直接执行截屏操作，此时确定用户权限信息对应的截屏处理方式，以根据截屏处理方式生成处理后的截屏图片，通过对用户的权限划分，确定对应的截屏处理方式，实现了在截屏时多样化的处理，使不同用户对同一界面进行截屏也具备差异性，同时满足了不同环境中对截屏图片处理的需求。

[0151] 当应用程序获得截屏授权指令时，根据当前用户的权限信息给出当前界面的截屏

界面。

[0152] 其中，截屏处理方式包括对待生成的截屏图片进行雾化处理，在底层添加包括公司LOGO的水印，屏蔽界面上的关键信息，以及生成白屏图片等。

[0153] 在上述任一项技术方案中，优选地，确定单元206还用于：确定当前界面的敏感信息；截屏装置200还包括：屏蔽单元216，用于对敏感信息执行屏蔽操作，以生成处理后的截屏图片。

[0154] 在该技术方案中，通过确定当前界面的敏感信息，并对敏感信息执行屏蔽操作，以生成处理后的截屏图片，防止了敏感信息的外泄，提升了截屏操作的安全性，并且细化了截屏效果。

[0155] 敏感信息包括公司的机密信息、用户的个人资料等。

[0156] 图3示出了根据本发明的实施例的终端的示意框图。

[0157] 如图3所示，根据本发明的实施例的终端300，包括上述任一项技术方案的所述的截屏装置200，因此，该终端300包括上述任一项技术方案的所述的截屏装置200的技术效果，在此不再赘述。

[0158] 图4示出了根据本发明的另一个实施例的截屏方法的示意流程图。

[0159] 如图4所示，根据本发明的另一个实施例的截屏方法，包括：步骤402，在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数；步骤404，将截屏状态参数发送至终端，以使终端根据截屏状态参数对截屏指令进行判断，以确定是否根据截屏指令进行截屏处理。

[0160] 在该技术方案中，服务器在接收到终端的登陆信息时，根据登陆信息确定对应的截屏状态参数，并将截屏状态参数发送至终端，以使终端在获取到截屏指令时，根据截屏状态参数对截屏指令进行判断，来确定是否进行截屏处理，通过应用程序与截屏状态参数的对应关系，在实现了服务器与终端交互的同时，根据不同的应用程序确定不同的截屏状态，实现了截屏指令处理的多样化，满足了用户对截屏不同处理方式的需求。

[0161] 在上述技术方案中，优选地，还包括：在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略；将截屏策略发送至终端，以使终端根据截屏策略确定截屏指令的执行方式。

[0162] 在该技术方案中，服务器在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略，并将截屏策略发送至终端，以使终端根据截屏策略进行具体的截屏操作，从而体现了用户截屏操作的差异化，满足了不同用户使用的需求。

[0163] 在上述任一项技术方案中，优选地，在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数前，还包括：预存应用程序对应的截屏状态参数。

[0164] 在该技术方案中，通过在服务器中预存对应的截屏状态参数，在终端访问服务器时就能够获得应用程序对应的截屏状态参数，减少了终端本地预设步骤，实现了区域化终端截屏管理，满足了办公的需求。

[0165] 图5示出了根据本发明的另一个实施例的截屏装置的示意框图。

[0166] 如图5所示，根据本发明的另一个实施例的截屏装置500，包括：确定单元502，用于在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数；发送单元504，用于将截屏状态参数发送至终端，以使终端根据截屏状态参数对截屏指令进行

判断，以确定是否根据截屏指令进行截屏处理。

[0167] 在该技术方案中，服务器在接收到终端的登陆信息时，根据登陆信息确定对应的截屏状态参数，并将截屏状态参数发送至终端，以使终端在获取到截屏指令时，根据截屏状态参数对截屏指令进行判断，来确定是否进行截屏处理，通过应用程序与截屏状态参数的对应关系，在实现了服务器与终端交互的同时，根据不同的应用程序确定不同的截屏状态，实现了截屏指令处理的多样化，满足了用户对截屏不同处理方式的需求。

[0168] 在上述技术方案中，优选地，确定单元502还用于：在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略；发送单元504还用于：将截屏策略发送至终端，以使终端根据截屏策略确定截屏指令的执行方式。

[0169] 在该技术方案中，服务器在接收到终端发送的应用程序的用户信息时，根据用户信息确定对应的截屏策略，并将截屏策略发送至终端，以使终端根据截屏策略进行具体的截屏操作，从而体现了用户截屏操作的差异化，满足了不同用户使用的需求。

[0170] 在上述任一项技术方案中，优选地，还包括：预存单元506，用于预存应用程序对应的截屏状态参数。

[0171] 在该技术方案中，通过在服务器中预存对应的截屏状态参数，在终端访问服务器时就能够获得应用程序对应的截屏状态参数，减少了终端本地预设步骤，实现了区域化终端截屏管理，满足了办公的需求。

[0172] 图6示出了根据本发明的实施例的服务器的示意框图。

[0173] 如图6所示，根据本发明的实施例的服务器600，包括上述任一项技术方案的所述的截屏装置500，因此，该服务器600包括上述任一项技术方案的所述的截屏装置500的技术效果，在此不再赘述。

[0174] 图7示出了根据本发明的一个实施例的截屏方案的示意流程图。

[0175] 如图7所示，根据本发明的一个实施例的截屏方案的示意流程图，包括：步骤702，修改android_sdk对应用程序进行注册；步骤704，应用服务器对截屏效果进行管理；步骤706，拦截截屏指令，以根据不同的角色显示不同的效果。

[0176] 在该技术方案中，应用程序管理服务器对终端用户进行权限划分和截屏策略管理，终端授权并触发具体的应用程序进行截屏拦截，应用程序接到截屏授权指令时，根据用户信息和当前界面生成合适的截屏图片。

[0177] 进一步地，应用程序管理服务器需要建造一个针对截屏控制的权限机制，服务器管理员可以对截屏具体信息进行灵活配置以满足不同用户不同功能对应不同的截屏效果；

[0178] 进一步地，终端设置截屏状态参数，在用户触发截屏动作时，手机终端根据截屏状态参数判断具体对哪个应用程序进行截屏授权，比如，android系统终端可以将SDK中surface.java的状态属性ture和flase修改为A、B、C、D、E等来代表不同的截屏状态。

[0179] 应用程序在安装时在终端注册一个服务，当终端截屏时触发该服务进行截屏拦截。

[0180] 进一步地，当应用程序获取到截屏授权指令时，根据用户信息与当前信息界面生成截屏图片。

[0181] 与现有技术相比，通过预设截屏状态参数与用户权限信息，防止了终端截屏传播敏感信息，同时细化了截屏效果，让截屏安全控制更人性化、并且更有科技感，并且本方案

不是在系统运行时就进行信息安全控制，而是在用户进行不安全操作时才进行安全控制，不但减轻系统负担，同时使用户感觉不到角色壁垒和歧视。

[0182] 图8示出了根据本发明的另一个实施例的截屏方案的示意流程图；

[0183] 如图8所示，根据本发明的另一个实施例的截屏方案，包括：步骤802，通过修改android_SDK_surface对应用程序的截屏操作进行注册。

[0184] 通过修改android_SDK_surface对截屏操作进行注册，能够获得多个截屏状态参数，满足不同截屏需求。

[0185] 图9示出了根据本发明的再一个实施例的截屏方案的示意流程图。

[0186] 如图9所示，根据本发明的再一个实施例的截屏方案的示意流程图，包括：步骤902，用户打开应用程序进行截屏操作；步骤904，SDK触发surface进行截屏拦截；步骤906，判断用户角色是否被授权，在判断结果为“是”时，进入步骤908，在判定结果为“否”时，进入步骤910；步骤908，进行正常截屏操作；步骤910，对用户截屏完的图片进行处理、进行底层水印绘制、屏蔽关键信息或白屏等。

[0187] 在该技术方案中，在拦截到截屏指令时，判断用户角色是否被授权，通过对用户的权限划分，确定对应的截屏处理方式，实现了在截屏时多样化的处理，使不同用户对同一界面进行截屏也具备差异性，同时满足了不同环境中对截屏图片处理的需求。

[0188] 图10示出了根据本发明的又一个实施例的截屏方案的示意图。

[0189] 如图10所示，终端和管理服务器之间进行交互操作，在服务器接收到终端发送的应用程序的登陆信息时，服务器向终端发送安全截屏水印，以使终端在接收到应用程序中任一界面的截屏指令时，在截屏图片底层添加截屏水印，从而能够明确表明截屏图片的出处，提升了截屏图片传播的安全性。

[0190] 图11与图12示出了根据本发明的又一个实施例的截屏方案的示意图。

[0191] 图11示出了接收到截屏指令时当前界面的界面信息，当前截屏为单据明细包括：单据编号：201214558787777、单据类型：差旅费报销、供应商：肖家波、金额：14140.0、报账人：肖建波、摘要：财务部报销差旅费，根据当前界面所属的应用程序确定对应的截屏状态参数，在截屏状态参数为允许处理后截屏时，根据用户的权限信息确定处理方式，比如，在检测到当前界面上具有敏感信息时(金额)，则将敏感信息进行屏蔽，生成处理后的截屏图片，如图12所示，从而防止了敏感信息外泄。

[0192] 以上结合附图详细说明了本发明的技术方案，考虑到相关技术中如何提高截屏控制的安全性的技术问题，本发明提出了一种新的截屏方案，通过在获取到对当前界面的截屏指令时，对截屏指令进行判断，以确定是否允许截屏，在判断结果为允许截屏时，则根据截屏指令生成截屏图片，在判断结果为不允许截屏时，则不执行截屏操作，通过对截屏指令进行判断，防止了具有敏感信息与保密信息的页面被截屏传播，提高了截屏操作的安全性，提升了用户的使用体验。

[0193] 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。

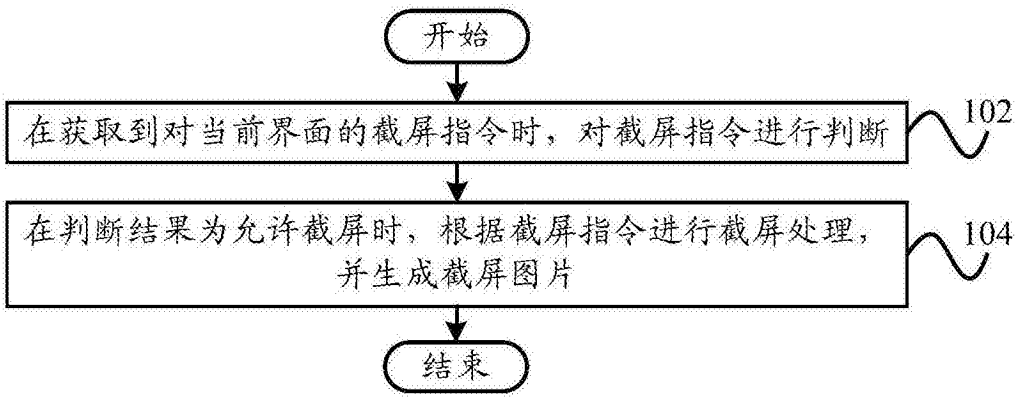

开始
在获取到对当前界面的截屏指令时，对截屏指令进行判断
102
在判断结果为允许截屏时，根据截屏指令进行截屏处理，并生成截屏图片
104
结束

图1


判断单元202
截屏处理单元204
确定单元206
预设单元208
修改单元210
检测单元212
执行单元214
屏蔽单元216
截屏装置200

图2


截屏装置200
终端300

图3

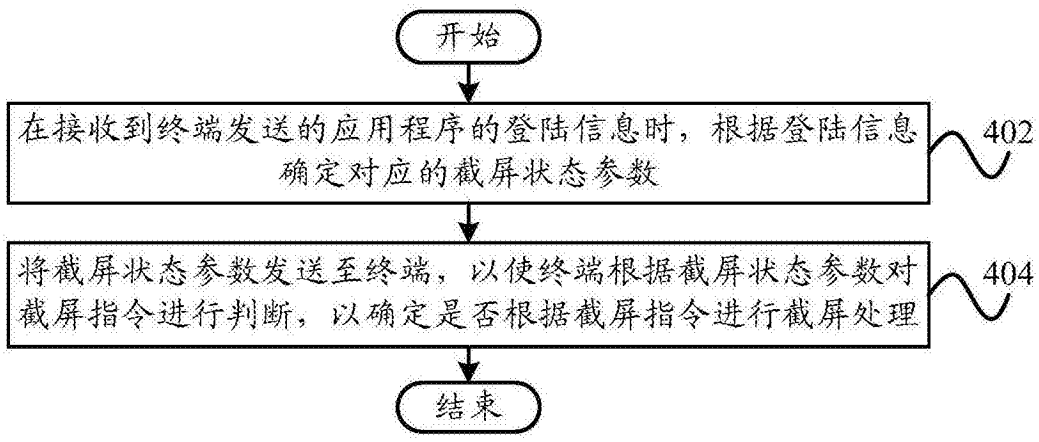

开始
在接收到终端发送的应用程序的登陆信息时，根据登陆信息确定对应的截屏状态参数
402
将截屏状态参数发送至终端，以使终端根据截屏状态参数对截屏指令进行判断，以确定是否根据截屏指令进行截屏处理
404
结束

图4


确定单元502
发送单元504
预存单元506
截屏装置500

图5

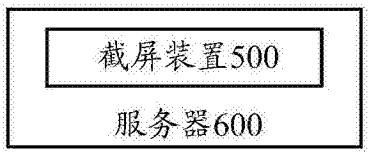

截屏装置500
服务器600

图6

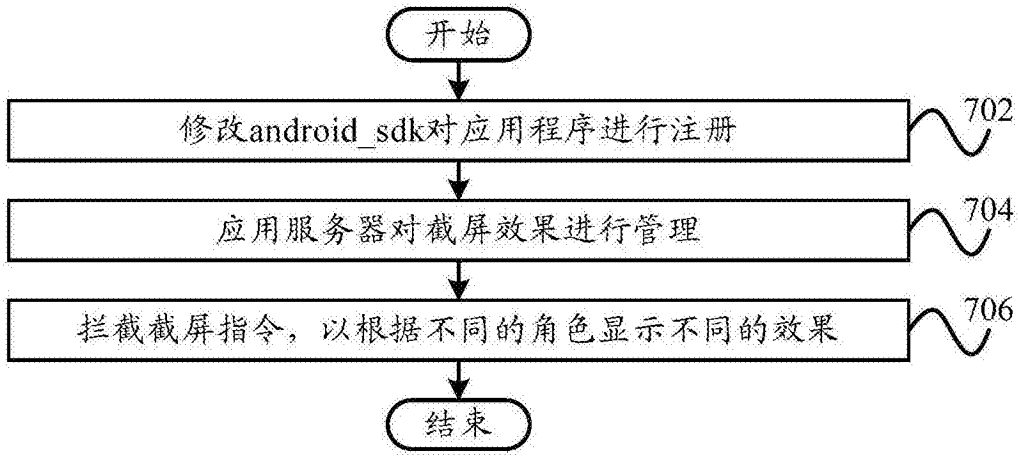

开始
修改android_sdk对应用程序进行注册
702
应用服务器对截屏效果进行管理
704
拦截截屏指令，以根据不同的角色显示不同的效果
706
结束

图7

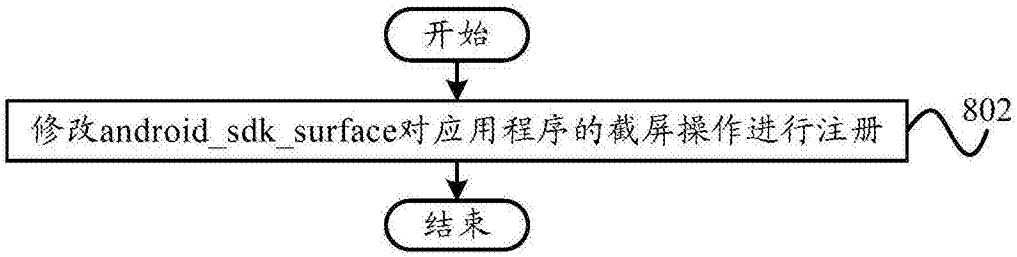

开始
修改android_sdk_surface对应用程序的截屏操作进行注册
802
结束

图8

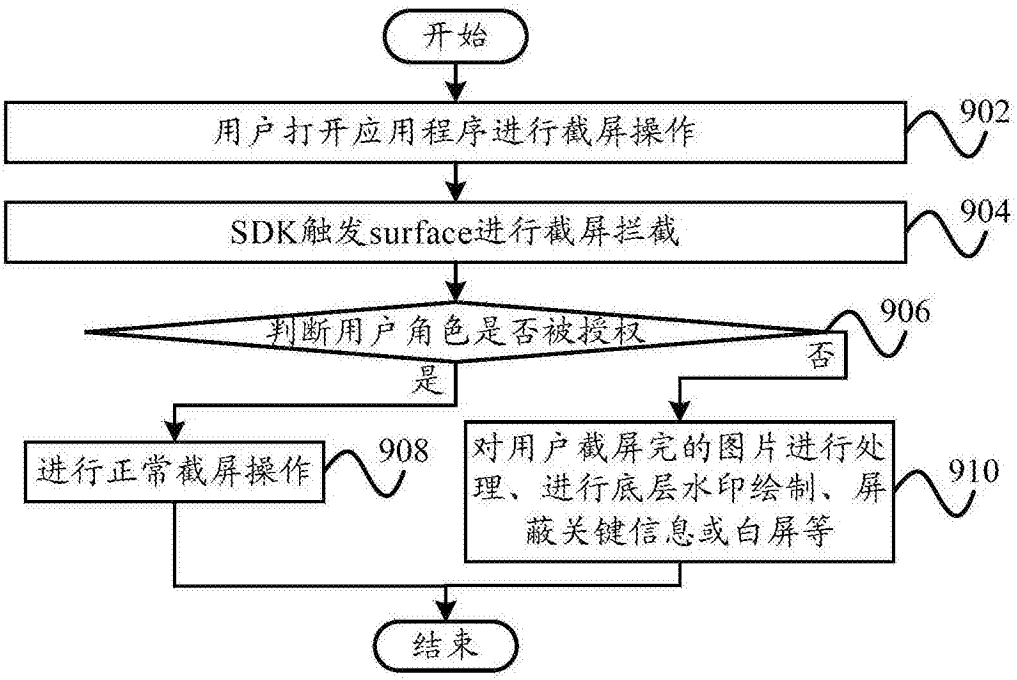

开始
用户打开应用程序进行截屏操作
902
SDK触发surface进行截屏拦截
904
判断用户角色是否被授权
906
否
是
进行正常截屏操作
908
对用户截屏完的图片进行处理、进行底层水印绘制、屏蔽关键信息或白屏等
910
结束

图9

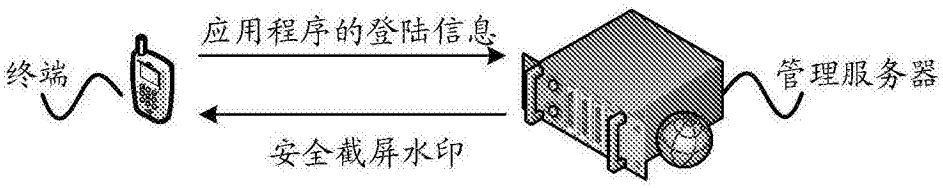

应用程序的登陆信息
终端
管理服务器
安全截屏水印

图10


单据明细
单据编号: 2012145587877777
单据类型: 差旅费报销
供 应 商: 肖家波
金 额: 14140.0
报 账 人: 肖建波
摘 要: 财务部报销差旅费
审批历史

图11


单据明细
单据编号: 2012145587877777
单据类型: 差旅费报销
供 应 商: 肖家波
金 额:
报 账 人: 肖建波
摘 要: 财务部报销差旅费
审批历史

图12