(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
2020 年 12 月 24 日 (24.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/253068 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2019/118599

(22) 国际申请日: 2019 年 11 月 14 日 (14.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910533846.4 2019年6月19日 (19.06.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 刘翔 (LIU, Xiang); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。 殷兆芳 (YIN, Zhaofang); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市龙华新区龙观东路83号荣群大厦9楼, Guangdong 518109 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) **Title:** SHARED FILE SECURITY MANAGEMENT METHOD AND APPARATUS, TERMINAL AND READABLE STORAGE MEDIUM

(54) **发明名称**: 共享文件安全管理方法、装置、终端及可读存储介质

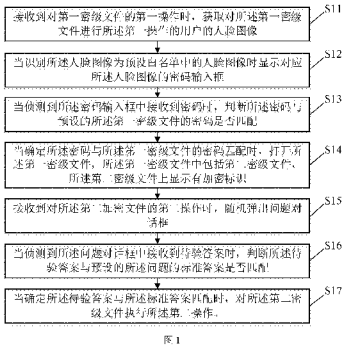

图 1

S11 When a first operation on a first security-level file is received, acquire a facial image of a user performing the first operation on the first security-level file

S12 When it is recognized that the facial image is a facial image in a preset white list, display a password input box corresponding to the facial image

S13 When it is detected that the password input box receives a password, determine whether the password matches a preset password of the first security-level file

S14 When it is determined that the password matches the password of the first security-level file, open the first security-level file, wherein the first security-level file comprises a second security-level file, and an encryption identifier is displayed on the second security-level file

S15 When a second operation on the second security-level file is received, a question dialog box randomly pops up

S16 When it is detected that the question dialog box receives an answer to be verified, determine whether the answer to be verified matches a preset standard answer to a question

S17 When it is determined that the answer to be verified matches the standard answer, execute the second operation on the second security-level file

(57) **Abstract:** Provided is a shared file security management method. The method comprises: acquiring a facial image of a user performing a first operation on a first security-level file; when the facial image is a facial image in a preset white list, displaying a password input box; when it is determined that a password in the password input box matches a password corresponding to a preset first security-level file, opening the first security-level file, wherein the first security-level file comprises a second security-level file; when a second operation on the second security-level file is received, a question dialog box randomly popping up; and when it is determined that an answer to be verified in the question dialog box matches a standard answer to a question, executing the second operation on the second security-level file. Further provided are a shared file security management apparatus, a terminal and a non-volatile computer-readable storage medium. According to the method, the security of the first security-level file in a shared disk is ensured by means of determining the facial image of the user, and at the same time, if the second security-level file in the first security-level file is operated, the security of the second security-level file is ensured by randomly displaying the question dialog box.

(57) **摘要**: 一种共享文件安全管理方法，包括：获取对第一密级文件进行第一操作的用户的人脸图像；当人脸图像为预设白名单中的人脸图像时显示密码输入框，判断密码输入框中的密码与预设的第一密级文件对应的密码匹配时，打开第一密级文件，第一密级文件中包括第二密级文件，当接收到对第二密级文件的第二操作时，随机弹出问题对话框；判断问题对话框中的待验答案与问题的标准答案匹配时，对第二密级文件执行第二操作。还提供一种共享文件安全管理装置、终端及非易失性计算机可读存储介质。所述方法通过判断用户的人脸图像保证共享盘中的第一密级文件的安全性，同时若对第一密级文件中的第二密级文件进行操作时，随机显示问题对话框来确保第二密级文件的安全性。

WO 2020/253068 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

共享文件安全管理方法、装置、终端及可读存储介质

本申请要求于 2019 年 06 月 19 日提交中国专利局，申请号为 201910533846.4 发明名称为“共享文件安全管理方法、装置、终端及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及云桌面办公技术领域，具体涉及一种共享文件安全管理方法、装置、终端及可读存储介质。

背景技术

随着通信技术的迅速发展，信息数据的传递越来越方便快捷，人们获取信息的路径和范围越来越广泛。信息安全性变得更加严峻。特别是项目组内部信息的安全性，如有同事请假不在，项目信息需要紧急处理，密码便会告知他人，由他人帮忙进行处理，那么此时就会存在项目信息安全隐患问题。特别是项目核心的技术文件，如果泄密，就会给公司带来巨大的风险，甚至造成巨大的经济损失。

虽可以通过对重要文件进行加密的方式来确保文件的安全性，但密码容易被泄露。尤其是对协同办公的情况下，无法保证共享文件的安全。

因此，如何在共享办公的环境下，保证密级等级高的文件的安全成为亟待解决的技术问题。

发明内容

鉴于以上内容，有必要提出一种共享文件安全管理方法、装置、终端及可读存储介质，通过判断用户的人脸图像保证共享盘中的第一密级文件的安全性，同时若对第一密级文件中的第二密级文件进行操作时，随机显示问题对话框来确保第二密级文件的安全性。

本申请的第一方面提供一种共享文件安全管理方法，应用于终端中，所述方法包括：

接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像；

当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框；

当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对

应的密码是否匹配；

当确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作；

接收到对所述第二密级文件的第二操作时，随机弹出问题对话框；

当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配；

当确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

本申请的第二方面提供一种共享文件安全管理装置，所述装置包括：

获取模块，用于接收到对第一密级文件的第一操作时， 获取对所述第一密级文件进行所述第一操作的用户的人脸图像；

显示模块，用于当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框；

第一判断模块，用于当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配；

打开模块，用于当所述第一判断模块确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作；

弹出模块，用于接收到对所述第二密级文件的第二操作时，随机弹出问题对话框；

第二判断模块，用于当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配；

执行模块，用于当所述第二判断模块确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

本申请的第三方面提供一种终端，所述终端包括处理器，所述处理器用于执行存储器中存储的至少一个计算机可读指令时实现所述共享文件安全管理方法。

本申请的第四方面提供一种非易失性计算机可读存储介质，所述非易失性计算机可读存储介质上存储有至少一个计算机可读指令，所述计算机可读指令被处理器执行时实现所述共享文件安全管理方法。

综上所述，本申请所述的共享文件安全管理方法、装置、终端及可读存储介质，首先通

过判断对第一密级文件进行第一操作的用户的人脸图像是否为白名单中的人脸图像，再通过验证对应所述人脸图形的密码输入框中接收到的密码的正确性，来双重确保共享盘中的第一密级文件的安全性；其次，第二密级文件是在第一密级文件中，只有正常打开了第一密级文件，才能显示出第二密级文件，且第二密级文件上具有密级标识，标识无操作权限的人员不可对第二密级文件进行第二操作；再次，当侦测到对第二密级文件的第二操作时，随机显示问题对话框，通过验证所述随机显示问题对话框中接收到待验答案与问题的标准答案之间的匹配度来确保第二密级文件的安全性。

附图说明

图 1 是本申请实施例一提供的共享文件安全管理方法的流程图。

图 2 是本申请实施例二提供的共享文件安全管理装置的结构图。

图 3 是本申请实施例三提供的终端的结构示意图。

如下具体实施方式将结合上述附图进一步说明本申请。

具体实施方式

为了能够更清楚地理解本申请的上述目的、特征和优点，下面结合附图和具体实施例对本申请进行详细描述。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。

实施例一

图 1 是本申请实施例一提供的共享文件安全管理方法的流程图。

在本实施例中，所述共享文件安全管理方法可以应用于终端中，对于需要进行共享文件安全管理的终端，可以直接在终端上集成本申请的方法所提供的共享文件安全管理的功能，或者以软件开发工具包（Software Development Kit，SKD）的形式运行在终端中。

如图 1 所示，所述共享文件安全管理方法具体包括以下步骤，根据不同的需求，该流程图中步骤的顺序可以改变，某些可以省略。

S11：接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像。

本实施例中，项目组可以使用共享云桌面、共享磁盘或者共享服务器存储大量的密级文件。不同的密级文件的密级等级不同，同一密级等级对应多个不同的密级文件。以两类密级等级为例进行说明，第一密级等级对应第一类密级文件，第二密级等级对应第二类密级文件，第一密级等级低于第二密级等级。

所述第一类密级文件称之为第一密级文件，第一密级文件是指一些不重要的文件，如网上直接下载的文件、程序性文件、展会上搜集的文件等。

所述第二类密级文件称之为第二密级文件，第二密级文件是指与项目组相关的核心文件，需要较强的保密性。

当用户预对第一密级文件进行第一操作时，终端接收到第一密级文件的第一操作指令，则获取用户的人脸图像，根据人脸图像显示不同的密码输入界面。

所述第一操作可以为打开操作。

S12：当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框。

本实施例中，终端先判断人脸图像是否为白名单中的人脸图像，在确定所述人脸图像为白名单中的人脸图像时，表明用户拥有对第一密级文件进行第一操作的角色权限，从而再对人脸图像进行识别，根据识别到的人脸图像显示不同的密码输入界面。

优选的，所述显示对应所述人脸图像的密码输入框包括：

识别所述人脸图像中的用户对应的角色权限；

当所述角色权限为第一角色权限时，直接对所述第一密级文件进行所述第一操作；

当所述角色权限为第二角色权限时，显示对应所述第二角色权限的密码输入框。

可以预先设置密码输入界面与对第一密级文件进行第一操作的用户的角色权限之间的对应关系。例如，当对第一密级文件进行第一操作的用户具有第一角色权限时，显示的第一密码输入界面上有 0 个密码输入框，即不需要输入密码即可直接打开第一密级文件；当对第一密级文件进行第一操作的用户具有第二角色权限时，显示的第二密码输入界面上有 1 个密码输入框。

所述拥有第一角色权限的人员可以包括：项目组领导、公司高层领导。

所述拥有第二角色权限的人员可以包括：项目组成员、公司知识产权人员中的一个或者多个。

本实施例中，对拥有第一角色权限的用户，例如，公司领导，想要查看第一密级文件的时候，可以不用输入密码，直接打开第一密级文件，节省了领导的时间；对拥有第二角色权限的用户，设置密码输入框，保证了文件的安全性。同时设置第一操作为打开操作，确保所有用户只能打开第一密级文件，而无法对第一密级文件进行删除或者复制。

S13：当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配。

本实施例中，可以预先建立一个数据库，数据库中记录了所有第一密级文件的密级等级

及预设的第一密级文件对应的密码，同时所述数据库中还关联了用户的人脸图像、用户的工号、用户的职位、用户的邮箱等。

当用户在所显示的密码输入框中输入了密码后，终端将所输入的密码与数据库中的预设的第一密级文件的密码进行匹配。当确定所述密码与预设的所述第一密级文件对应的密码匹配时，认为所输入的密码正确；当确定所述密码与预设的所述第一密级文件对应的密码不匹配时，认为所输入的密码错误。

优选的，所述判断所述密码与预设的所述第一密级文件对应的密码是否匹配包括：

获取与所述人脸图像对应的所述第一密级文件的目标密码，不同的人脸图形对应所述第一密级文件的目标密码不同；

判断所述密码与所述目标密码是否匹配。

示例性的，假设数据库中记录的预设的对应所述第一密级文件的密码为 A，人脸图像对应的用户 1，在密码输入框中输入密码 A，则终端确定所输入的密码正确；如果用户 1 在密码输入框中输入密码 B，则终端确定所输入的密码错误。

本实施例中，根据不同的第二角色权限的用户设置打开第一密级的密码不同，进一步加强了共享文件的安全的管理。

S14：当确定所述密码与所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识。

本实施例中，当确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开第一密级文件，供用户对所述第一密级文件进行第一操作。

本实施例中，所述第一密级文件中存放有多个子文件，所述子文件有些是加密文件，有些是非加密文件，将加密文件称之为第二密级文件。

第二密级文件上还显示有预先设置的加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作，即所述加密标识用以提示该第二密级文件是加密文件，无角色权限的用户不要点击或者触摸第二密级文件。

当确定所述密码与预设的所述第一密级文件对应的密码不匹配时，可以重新执行 S13，也可以直接结束流程。

S15：接收到对所述第二密级文件的第二操作时，随机弹出问题对话框。

本实施例中，当用户预对第二密级文件进行第二操作时，终端接收到第二密级文件的第二操作指令，则弹出问题对话框。所述第二操作可以为：打开操作、修改操作、复制操作。

所述第二密级文件是指一些非常重要的文件，例如，项目文件代码、项目试验数据、领导决策文件、项目计划书等文件。所述第二密级文件的密级等级高于第一密级文件的密级等

级。要想打开第二密级文件必须先打开第一密级等级文件。

优选的，所述接收到对所述第二密级文件的第二操作时，随机弹出问题对话框包括：

提取所述第二密级文件的文件内容中的多个第一关键词；

根据每个所述第一关键词首次出现的位置顺序确定所述每个第一关键词的编号；

采用随机数生成算法生成一个随机数；

根据所述随机数与编号之间的对应关系筛选出对应所述随机数的第一目标关键词；

弹出与所述第一目标关键词对应的问题对话框，所述问题对话框中显示有与所述第一目标关键词对应的问题。

本实施例中，根据第二密级文件的文件内容随机产生对应所述第二密级文件的问题，不同的第二密级文件对应不同的问题，不同的问题对应不同的答案。

S16：当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配。

用户根据弹出的问题对话框中的问题输入答案，然后判断所述答案与数据库中预先设置的对应所述问题的标准答案是否匹配。

优选的，所述判断所述待验答案与预设的所述问题的标准答案是否匹配包括：

根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度；

获取所述第二密级文件对应的预设匹配度阈值；

判断所述匹配度是否大于所述匹配度阈值；

当所述匹配度大于或者等于所述匹配度阈值时，确定所述待验答案与所述标准答案匹配；

当所述匹配度小于所述匹配度阈值时，确定所述待验答案与所述标准答案不匹配。

用户在问题对话框中输入的答案称之为待验答案。

本实施例中，可以预先为每一个第二密级文件对应设置一个匹配度阈值，所述匹配度阈值，用以评判用户在问题对话框中输入的答案与问题的标准答案之间的匹配度的临界值。例如，第二密级文件的密级等级为绝密时，对应的匹配度阈值可以设置为 100%；第二密级文件的密级等级为机密时，对应的匹配度阈值可以设置为 90%；第二密级文件的密级等级为秘密时，对应的匹配度阈值可以设置为 80%。若匹配度大于匹配度阈值，则表明待验答案为标准答案或者接近标准答案，即可确定待验答案为正确答案。若匹配度小于匹配度阈值，则表明待验答案与标准答案差距较大，确定待验答案不为正确答案。

通过设置匹配度阈值，再判断待验答案与标准答案之间的匹配度与匹配度阈值之间的大小关系，来确定待验答案的正确性与否。而无需严格对照标准答案来校验用户输入的答案的正确性，从而可以在确保第二密级文件高安全性的前提下，可以一定程度上的解放用户的记

忆力。

优选的，所述根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度包括：

提取所述待验答案中的预设第二关键词；

提取所述标准答案中的预设第三关键词；

统计所述预设第二关键词中与所述第三关键词相同的关键词的第一个数；

计算所述第一个数占所述预设第三关键词的第二个数的比例；

将所述比例作为所述待验答案与所述标准答案之间的匹配度。

示例性的，若所输入的回答问题的待验答案为“参加项目的项目组成员包括：第三关键词 J、第三关键词 K、第三关键词 L、第三关键词 N”，预设的标准答案为“参加项目的项目组成员包括：第二关键词 J、第二关键词 K、第二关键词 M、第二关键词 N”，识别出具有相同的关键词为“J、K、N”，相同的关键词的第一个数为 3，标准答案的第二关键词的第二个数为 4，计算所统计的相同的关键词个数占所预设的答案中关键词总个数的比例为 75%，则待验答案与所述标准答案之间的匹配度为 75%。

由于问题是按照第二密级文件的文件内容进行设置的，根据第二密级文件的密级等级，设置的问题的难易程度也不同，如果第二密级文件的密级等级较高，对该第二密级文件设置的问题相对较难，如果第二密级文件的密级等级较低，对该第二密级文件设置的问题相对较简单。对每个第二密级文件会设置多个问题，当侦测到对第二密级文件的第二操作时，随机弹出问题对话框。通过随机弹出问题对话框，进一步的保证了第二密级文件的安全性，如果没有参与第二密级文件对应的项目，或者对所述项目不了解的人员，是无法打开第二密级文件的。

S17：当判断所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

本实施例中，在判断所述待验答案与数据库中预设的所述问题的标准答案匹配时，可以按照用户的所述第二操作来对所述第二密级文件执行相应的功能。比如，第二操作是打开操作时，执行打开第二密级文件的功能。又如，第二操作是复制操作时，执行复制第二密级文件的功能。

当判断所述待验答案与所述标准答案不匹配时，可以继续执行 S16，也可以直接结束流程。

进一步的，在判断所述待验答案与所述标准答案不匹配之后，所述方法还包括：

再次随机显示问题对话框；

当判断再次显示的问题对话框中的待验答案与标准答案之间不匹配时，将所述人脸图像发送给审核者进行审核；

当接收到所述审核者的审核结果为所述人脸图像对应的人员不具有对所述第二密级文件进行操作权限的人员时，将所述人脸图像移除所述白名单中。

本实施例中，第一次随机显示一个问题对话框，若问题对话框中的待验答案与标准答案不匹配时，再第二次随机显示一个问题对话框，若问题对话框中的待验答案与标准答案仍不匹配时，终端将人脸图像发送给审核者进行审核，以判断人脸图像对应的用户是否具有对第二密级文件进行第二操作的操作权限。当审核的结果为不具有操作第二密级文件的操作权限时，将人脸图像从白名单中移至黑名单中。因为第二密级文件上具有密级标识，已经提示过不具有操作权限的用户不可以对第二密级文件进行第二操作，倘若该用户两次在问题对话框中输入的密码均不对时，可以认为该用户不遵守公司制度或者该用户可能想窃取第二密级文，故将该用户直接拉黑，进一步确保了第一密级文件和第二密级文件的安全性。

综上所述，本申请所述共享文件安全管理方法，首先通过判断对第一密级文件进行第一操作的用户的人脸图像是否为白名单中的人脸图像，再通过验证对应所述人脸图形的密码输入框中接收到的密码的正确性，来双重确保共享盘中的第一密级文件的安全性；其次，第二密级文件是在第一密级文件中，只有正常打开了第一密级文件，才能显示出第二密级文件，且第二密级文件上具有密级标识，标识无操作权限的人员不可对第二密级文件进行第二操作；再次，当侦测到对第二密级文件的第二操作时，随机显示问题对话框，通过验证所述随机显示问题对话框中接收到待验答案与问题的标准答案之间的匹配度来确保第二密级文件的安全性。

实施例二

图 2 是本申请实施例二提供的共享文件安全管理装置的结构图。

在一些实施例中，所述共享文件安全管理装置 20 可以包括多个由程序代码段所组成的功能模块。所述共享文件安全管理装置 20 中的各个程序段的程序代码可以存储于终端的存储器中，并由至少一个处理器所执行，以执行（详见图 1 描述）对共享文件进行安全管理。

本实施例中，所述共享文件安全管理装置 20 根据其所执行的功能，可以被划分为多个功能模块。所述功能模块可以包括：获取模块 201、显示模块 202、第一判断模块 203、打开模块 204、弹出模块 205、第二判断模块 206、执行模块 207 及移除模块 208。本申请所称的模块是指一种能够被至少一个处理器所执行并且能够完成固定功能的一系列计算机可读指令段，其存储在存储器中。在本实施例中，关于各模块的功能将在后续的实施例中详述。

获取模块 201，用于接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像。

本实施例中，项目组可以使用共享云桌面、共享磁盘或者共享服务器存储大量的密级文件。不同的密级文件的密级等级不同，同一密级等级对应多个不同的密级文件。以两类密级等级为例进行说明，第一密级等级对应第一类密级文件，第二密级等级对应第二类密级文件，第一密级等级低于第二密级等级。

所述第一类密级文件称之为第一密级文件，第一密级文件是指一些不重要的文件，如网上直接下载的文件、程序性文件、展会上搜集的文件等。

所述第二类密级文件称之为第二密级文件，第二密级文件是指与项目组相关的核心文件，需要较强的保密性。

当用户预对第一密级文件进行第一操作时，终端接收到第一密级文件的第一操作指令，则获取用户的人脸图像，根据人脸图像显示不同的密码输入界面。

所述第一操作可以为打开操作。

显示模块 202，用于当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框。

本实施例中，终端先判断人脸图像是否为白名单中的人脸图像，在确定所述人脸图像为白名单中的人脸图像时，表明用户拥有对第一密级文件进行第一操作的角色权限，从而再对人脸图像进行识别，根据识别到的人脸图像显示不同的密码输入界面。

优选的，所述显示模块 202 显示对应所述人脸图像的密码输入框包括：

识别所述人脸图像中的用户对应的角色权限；

当所述角色权限为第一角色权限时，直接对所述第一密级文件进行所述第一操作；

当所述角色权限为第二角色权限时，显示对应所述第二角色权限的密码输入框。

可以预先设置密码输入界面与对第一密级文件进行第一操作的用户的角色权限之间的对应关系。例如，当对第一密级文件进行第一操作的用户具有第一角色权限时，显示的第一密码输入界面上有 0 个密码输入框，即不需要输入密码即可直接打开第一密级文件；当对第一密级文件进行第一操作的用户具有第二角色权限时，显示的第二密码输入界面上有 1 个密码输入框。

所述拥有第一角色权限的人员可以包括：项目组领导、公司高层领导。

所述拥有第二角色权限的人员可以包括：项目组成员中、公司知识产权人员中的一个或者多个。

本实施例中，对拥有第一角色权限的用户，例如，公司领导，想要查看第一密级文件的

时候，可以不用输入密码，直接打开第一密级文件，节省了领导的时间；对拥有第二角色权限的用户，设置密码输入框，保证了文件的安全性。同时设置第一操作为打开操作，确保所有用户只能打开第一密级文件，而无法对第一密级文件进行删除或者复制。

第一判断模块 203，用于当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配。

本实施例中，可以预先建立一个数据库，数据库中记录了所有第一密级文件的密级等级及预设的第一密级文件对应的密码，同时所述数据库中还关联了用户的人脸图像、用户的工号、用户的职位、用户的邮箱等。

当用户在所显示的密码输入框中输入了密码后，终端将所输入的密码与数据库中的预设的第一密级文件的密码进行匹配。当确定所述密码与预设的所述第一密级文件对应的密码匹配时，认为所输入的密码正确；当确定所述密码与预设的所述第一密级文件对应的密码不匹配时，认为所输入的密码错误。

优选的，所述第一判断模块 203 判断所述密码与预设的所述第一密级文件对应的密码是否匹配包括：

获取与所述人脸图像对应的所述第一密级文件的目标密码，不同的人脸图形对应所述第一密级文件的目标密码不同；

判断所述密码与所述目标密码是否匹配。

示例性的，假设数据库中记录的预设的对应所述第一密级文件的密码为 A，人脸图像对应的用户 1，在密码输入框中输入密码 A，则终端确定所输入的密码正确；如果用户 1 在密码输入框中输入密码 B，则终端确定所输入的密码错误。

本实施例中，根据不同的第二角色权限的用户设置打开第一密级的密码不同，进一步加强了共享文件的安全的管理。

打开模块 204，用于当所述第一判断模块 203 确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识。

本实施例中，当确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开第一密级文件，供用户对所述第一密级文件进行第一操作。

本实施例中，所述第一密级文件中存放有多个子文件，所述子文件有些是加密文件，有些是非加密文件，将加密文件称之为第二密级文件。

第二密级文件上还显示有预先设置的加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作，即所述加密标识用以提

示该第二密级文件是加密文件，无角色权限的用户不要点击或者触摸第二密级文件。

弹出模块 205，用于接收到对所述第二密级文件的第二操作时，随机弹出问题对话框。

本实施例中，当用户预对第二密级文件进行第二操作时，终端接收到第二密级文件的第二操作指令，则弹出问题对话框。所述第二操作可以为：打开操作、修改操作、复制操作。

所述第二密级文件是指一些非常重要的文件，例如，项目文件代码、项目试验数据、领导决策文件、项目计划书等文件。所述第二密级文件的密级等级高于第一密级文件的密级等级。要想打开第二密级文件必须先打开第一密级等级文件。

优选的，所述弹出模块 205 接收到对所述第二密级文件的第二操作时，随机弹出问题对话框包括：

提取所述第二密级文件的文件内容中的多个第一关键词；

根据所述多个第一关键词出现的位置确定所述多个第一关键词的编号；

采用随机数生成算法生成一个随机数；

根据所述随机数与编号之间的对应关系筛选出对应所述随机数的第一目标关键词；

弹出与所述第一目标关键词对应的问题对话框，所述问题对话框中显示有与所述第一目标关键词对应的问题。

本实施例中，根据第二密级文件的文件内容随机产生对应所述第二密级文件的问题，不同的第二密级文件对应不同的问题，不同的问题对应不同的答案。

第二判断模块 206，用于当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配。

用户根据弹出的问题对话框中的问题输入答案，然后判断所述答案与数据库中预先设置的对应所述问题的标准答案是否匹配。

优选的，所述第二判断模块 206 判断所述待验答案与预设的所述问题的标准答案是否匹配包括：

根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度；

获取所述第二密级文件对应的预设匹配度阈值；

判断所述匹配度是否大于所述匹配度阈值；

当所述匹配度大于或者等于所述匹配度阈值时，确定所述待验答案与所述标准答案匹配；

当所述匹配度小于所述匹配度阈值时，确定所述待验答案与所述标准答案不匹配。

用户在问题对话框中输入的答案称之为待验答案。

本实施例中，可以预先为每一个第二密级文件对应设置一个匹配度阈值，所述匹配度阈值，用以评判用户在问题对话框中输入的答案与问题的标准答案之间的匹配度的临界值。例

如，第二密级文件的密级等级为绝密时，对应的匹配度阈值可以设置为 100%；第二密级文件的密级等级为机密时，对应的匹配度阈值可以设置为 90%；第二密级文件的密级等级为秘密时，对应的匹配度阈值可以设置为 80%。若匹配度大于匹配度阈值，则表明待验答案为标准答案或者接近标准答案，即可确定待验答案为正确答案。若匹配度小于匹配度阈值，则表明待验答案与标准答案差距较大，确定待验答案不为正确答案。

通过设置匹配度阈值，再判断待验答案与标准答案之间的匹配度与匹配度阈值之间的大小关系，来确定待验答案的正确性与否。而无需严格对照标准答案来校验用户输入的答案的正确性，从而可以在确保第二密级文件高安全性的前提下，可以一定程度上的解放用户的记忆力。

优选的，所述根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度包括：

提取所述待验答案中的预设第二关键词；

提取所述标准答案中的预设第三关键词；

统计所述预设第二关键词中与所述第三关键词相同的关键词的第一个数；

计算所述第一个数占所述预设第三关键词的第二个数的比例；

将所述比例作为所述待验答案与所述标准答案之间的匹配度。

示例性的，若所输入的回答问题的待验答案为“参加项目的项目组成员包括：第三关键词 J、第三关键词 K、第三关键词 L、第三关键词 N”，预设的标准答案为“参加项目的项目组成员包括：第二关键词 J、第二关键词 K、第二关键词 M、第二关键词 N”，识别出具有相同的关键词为“J、K、N”，相同的关键词的第一个数为 3，标准答案的第二关键词的第二个数为 4，计算所统计的相同的关键词个数占所预设的答案中关键词总个数的比例为 75%，则待验答案与所述标准答案之间的匹配度为 75%。

由于问题是按照第二密级文件的文件内容进行设置的，根据第二密级文件的密级等级，设置的问题的难易程度也不同，如果第二密级文件的密级等级较高，对该第二密级文件设置的问题相对较难，如果第二密级文件的密级等级较低，对该第二密级文件设置的问题相对较简单。对每个第二密级文件会设置多个问题，当侦测到对第二密级文件的第二操作时，随机弹出问题对话框。通过随机弹出问题对话框，进一步的保证了第二密级文件的安全性，如果没有参与第二密级文件对应的项目，或者对所述项目不了解的人员，是无法打开第二密级文件的。

所述第二判断模块 206，还用于当判断所述待验答案与所述标准答案不匹配时，可以继续运行所述第二判断模块 206，也可以直接结束流程。

执行模块 207，用于当所述第二判断模块 206 确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

本实施例中，在判断所述待验答案与数据库中预设的所述问题的标准答案匹配时，可以按照用户的所述第二操作来对所述第二密级文件执行相应的功能。比如，第二操作是打开操作时，执行打开第二密级文件的功能。又如，第二操作是复制操作时，执行复制第二密级文件的功能。

进一步的，在所述第二判断模块 206 判断所述待验答案与所述标准答案不匹配之后，所述共享文件安全管理装置 20 还包括：

所述显示模块 202，还用于再次随机显示问题对话框；

所述第二判断模块 206，还用于当判断再次显示的问题对话框中的待验答案与标准答案之间不匹配时，将所述人脸图像发送给审核者进行审核；

移除模块 208，用于当接收到所述审核者的审核结果为所述人脸图像对应的人员不具有对所述第二密级文件进行操作权限的人员时，将所述人脸图像移除所述白名单中。

本实施例中，第一次随机显示一个问题对话框，若问题对话框中的待验答案与标准答案不匹配时，再第二次随机显示一个问题对话框，若问题对话框中的待验答案与标准答案仍不匹配时，终端将人脸图像发送给审核者进行审核，以判断人脸图像对应的用户是否具有对第二密级文件进行第二操作的操作权限。当审核的结果为不具有操作第二密级文件的操作权限时，将人脸图像从白名单中移至黑名单中。因为第二密级文件上具有密级标识，已经提示过不具有操作权限的用户不可以对第二密级文件进行第二操作，倘若该用户两次在问题对话框中输入的密码均不对时，可以认为该用户不遵守公司制度或者该用户可能想窃取第二密级文，故将该用户直接拉黑，进一步确保了第一密级文件和第二密级文件的安全性。

综上所述，本申请所述共享文件安全管理装置，首先通过判断对第一密级文件进行第一操作的用户的人脸图像是否为白名单中的人脸图像，再通过验证对应所述人脸图形的密码输入框中接收到的密码的正确性，来双重确保共享盘中的第一密级文件的安全性；其次，第二密级文件是在第一密级文件中，只有正常打开了第一密级文件，才能显示出第二密级文件，且第二密级文件上具有密级标识，标识无操作权限的人员不可对第二密级文件进行第二操作；再次，当侦测到对第二密级文件的第二操作时，随机显示问题对话框，通过验证所述随机显示问题对话框中接收到待验答案与问题的标准答案之间的匹配度来确保第二密级文件的安全性。

实施例三

参阅图 3 所示，为本申请实施例三提供的终端的结构示意图。在本申请较佳实施例中，所述终端 3 包括存储器 31、至少一个处理器 32、至少一条通信总线 33 及收发器 34。

本领域技术人员应该了解，图 3 示出的终端的结构并不构成本申请实施例的限定，既可以是总线型结构，也可以是星形结构，所述终端 3 还可以包括比图示更多或更少的其他硬件或者软件，或者不同的部件布置。

在一些实施例中，所述终端 3 包括一种能够按照事先设定或存储的指令，自动进行数值计算和/或信息处理的终端，其硬件包括但不限于微处理器、专用集成电路、可编程门阵列、数字处理器及嵌入式设备等。所述终端 3 还可包括客户设备，所述客户设备包括但不限于任何一种可与客户通过键盘、鼠标、遥控器、触摸板或声控设备等方式进行人机交互的电子产品，例如，个人计算机、平板电脑、智能手机、数码相机等。

需要说明的是，所述终端 3 仅为举例，其他现有的或今后可能出现的电子产品如可适应于本申请，也应包含在本申请的保护范围以内，并以引用方式包含于此。

在一些实施例中，所述存储器 31 用于存储程序代码和各种数据，例如安装在所述终端 3 中的共享文件安全管理装置 20，并在终端 3 的运行过程中实现高速、自动地完成程序或数据的存取。所述存储器 31 包括只读存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable Read-Only Memory，PROM）、可擦除可编程只读存储器（Erasable Programmable Read-Only Memory，EPROM）、一次可编程只读存储器（One-time Programmable Read-Only Memory，OTPROM）、电子擦除式可复写只读存储器（Electrically-Erasable Programmable Read-Only Memory，EEPROM）、只读光盘（Compact Disc Read-Only Memory，CD-ROM）或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的非易失性计算机可读的任何其他介质。

在一些实施例中，所述至少一个处理器 32 可以由集成电路组成，例如可以由单个封装的集成电路所组成，也可以是由多个相同功能或不同功能封装的集成电路所组成，包括一个或者多个中央处理器（Central Processing unit，CPU）、微处理器、数字处理芯片、图形处理器及各种控制芯片的组合等。所述至少一个处理器 32 是所述终端 3 的控制核心（Control Unit），利用各种接口和线路连接整个终端 3 的各个部件，通过运行或执行存储在所述存储器 31 内的程序或者模块，以及调用存储在所述存储器 31 内的数据，以执行终端 3 的各种功能和处理数据，例如执行共享文件安全管理的功能。

在一些实施例中，所述至少一条通信总线 33 被设置为实现所述存储器 31 以及所述至少一个处理器 32 等之间的连接通信。

尽管未示出，所述终端 3 还可以包括给各个部件供电的电源（比如电池），优选的，电

源可以通过电源管理装置与所述至少一个处理器 32 逻辑相连，从而通过电源管理装置实现管理充电、放电、以及功耗管理等功能。电源还可以包括一个或一个以上的直流或交流电源、再充电装置、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。所述终端 3 还可以包括多种传感器、蓝牙模块、Wi-Fi 模块等，在此不再赘述。

应该了解，所述实施例仅为说明之用，在专利申请范围上并不受此结构的限制。

上述以软件功能模块的形式实现的集成的单元，可以存储在一个非易失性计算机可读存储介质中。上述软件功能模块包括若干指令用以使得一台计算机设备（可以是个人计算机，终端，或者网络设备等）或处理器（processor）执行本申请各个实施例所述方法的部分。

在进一步的实施例中，结合图 2，所述至少一个处理器 32 可执行所述终端 3 的操作装置以及安装的各类应用程序（如所述的共享文件安全管理装置 20）、程序代码等，例如，上述的各个模块。

所述存储器 31 中存储有程序代码，且所述至少一个处理器 32 可调用所述存储器 31 中存储的程序代码以执行相关的功能。例如，图 2 中所述的各个模块是存储在所述存储器 31 中的程序代码，并由所述至少一个处理器 32 所执行，从而实现所述各个模块的功能以达到共享文件安全管理的目的。

在本申请的一个实施例中，所述存储器 31 存储多个指令，所述多个指令被所述至少一个处理器 32 所执行以实现共享文件安全的管理。

具体地，所述至少一个处理器 32 对上述指令的具体实现方法可参考图 1 对应实施例中相关步骤的描述，在此不赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

最后应说明的是，以上实施例仅用以说明本申请的技术方案而非限制，尽管参照较佳实施例对本申请进行了详细说明，本领域的普通技术人员应当理解，可以对本申请的技术方案进行修改或等同替换，而不脱离本申请技术方案的精神和范围。

权 利 要 求 书

1. 一种共享文件安全管理方法，应用于终端中，其特征在于，所述方法包括：

接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像；

当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框；

当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配；

当确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作；

接收到对所述第二密级文件的第二操作时，随机弹出问题对话框；

当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配；

当确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

2. 如权利要求 1 所述的方法，其特征在于，所述当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框包括：

识别所述人脸图像中的用户对应的角色权限；

当所述角色权限为第一角色权限时，直接对所述第一密级文件进行所述第一操作；

当所述角色权限为第二角色权限时，显示对应所述第二角色权限的密码输入框。

3. 如权利要求 1 所述的方法，其特征在于，所述判断所述密码与预设的所述第一密级文件对应的密码是否匹配包括：

获取与所述人脸图像对应的所述第一密级文件的目标密码，不同的人脸图形对应所述第一密级文件的目标密码不同；

判断所述密码与所述目标密码是否匹配。

4. 如权利要求 1 所述的方法，其特征在于，所述接收到对所述第二密级文件的第二操作时，随机弹出问题对话框包括：

提取所述第二密级文件的文件内容中的多个第一关键词；

根据每个所述第一关键词首次出现的位置顺序确定所述每个第一关键词的编号；

采用随机数生成算法生成一个随机数；

根据所述随机数与编号之间的对应关系筛选出对应所述随机数的第一目标关键词；

弹出与所述第一目标关键词对应的问题对话框，所述问题对话框中显示有与所述第一目标关键词对应的问题。

5. 如权利要求 1 所述的方法，其特征在于，所述判断所述待验答案与所述问题的标准答案是否匹配包括：

根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度；

获取所述第二密级文件对应的预设匹配度阈值；

判断所述匹配度是否大于所述匹配度阈值；

当所述匹配度大于或者等于所述匹配度阈值时，确定所述待验答案与所述标准答案匹配；

当所述匹配度小于所述匹配度阈值时，确定所述待验答案与所述标准答案不匹配。

6. 如权利要求 5 所述的方法，其特征在于，所述根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度包括：

提取所述待验答案中的预设第二关键词；

提取所述标准答案中的预设第三关键词；

统计所述预设第二关键词中与所述第三关键词相同的关键词的第一个数；

计算所述第一个数占所述预设第三关键词的第二个数的比例；

将所述比例作为所述待验答案与所述标准答案之间的匹配度。

7. 如权利要求 1 所述的方法，其特征在于，在判断所述待验答案与所述标准答案不匹配之后，所述方法还包括：

再次随机显示问题对话框；

当判断再次显示的问题对话框中的待验答案与标准答案之间不匹配时，将所述人脸图像发送给审核者进行审核；

当接收到所述审核者的审核结果为所述人脸图像对应的人员不具有对所述第二密级文件进行操作权限的人员时，将所述人脸图像移除所述白名单中。

8. 一种共享文件安全管理装置，运行于终端中，其特征在于，所述装置包括：

获取模块，用于接收到对第一密级文件的第一操作时， 获取对所述第一密级文件进行所述第一操作的用户的人脸图像；

显示模块，用于当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框；

第一判断模块，用于当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配；

打开模块，用于当所述第一判断模块确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作；

弹出模块，用于接收到对所述第二密级文件的第二操作时，随机弹出问题对话框；

第二判断模块，用于当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配；

执行模块，用于当所述第二判断模块确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

9. 一种终端，其特征在于，所述终端包括处理器，所述处理器用于执行存储器中存储的至少一个计算机可读指令时实现以下步骤：

接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像；

当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框；

当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配；

当确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作；

接收到对所述第二密级文件的第二操作时，随机弹出问题对话框；

当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配；

当确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

10. 如权利要求 9 所述的终端，其特征在于，所述处理器执行所述至少一个计算机可读指令以实现所述显示对应所述人脸图像的密码输入框时，包括：

识别所述人脸图像中的用户对应的角色权限；

当所述角色权限为第一角色权限时，直接对所述第一密级文件进行所述第一操作；

当所述角色权限为第二角色权限时，显示对应所述第二角色权限的密码输入框。

11. 如权利要求 9 所述的终端，其特征在于，所述处理器执行所述至少一个计算机可读

指令以实现所述判断所述密码与预设的所述第一密级文件对应的密码是否匹配时，包括：

获取与所述人脸图像对应的所述第一密级文件的目标密码，不同的人脸图形对应所述第一密级文件的目标密码不同；

判断所述密码与所述目标密码是否匹配。

12. 如权利要求 9 所述的终端，其特征在于，所述处理器执行所述至少一个计算机可读指令以实现随机弹出问题对话框时，包括：

提取所述第二密级文件的文件内容中的多个第一关键词；

根据每个所述第一关键词首次出现的位置顺序确定所述每个第一关键词的编号；

采用随机数生成算法生成一个随机数；

根据所述随机数与编号之间的对应关系筛选出对应所述随机数的第一目标关键词；

弹出与所述第一目标关键词对应的问题对话框，所述问题对话框中显示有与所述第一目标关键词对应的问题。

13. 如权利要求 9 至 12 中任意一项所述的终端，其特征在于，所述处理器执行所述至少一个计算机可读指令以实现所述判断所述待验答案与所述问题的标准答案是否匹配时，包括：

根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度；

获取所述第二密级文件对应的预设匹配度阈值；

判断所述匹配度是否大于所述匹配度阈值；

当所述匹配度大于或者等于所述匹配度阈值时，确定所述待验答案与所述标准答案匹配；

当所述匹配度小于所述匹配度阈值时，确定所述待验答案与所述标准答案不匹配。

14. 如权利要求 13 所述的终端，其特征在于，所述处理器执行所述至少一个计算机可读指令以实现所述根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度时，包括：

提取所述待验答案中的预设第二关键词；

提取所述标准答案中的预设第三关键词；

统计所述预设第二关键词中与所述第三关键词相同的关键词的第一个数；

计算所述第一个数占所述预设第三关键词的第二个数的比例；

将所述比例作为所述待验答案与所述标准答案之间的匹配度。

15. 如权利要求 9 所述的终端，其特征在于，在判断所述待验答案与所述标准答案不匹配之后，所述处理器执行所述至少一个计算机可读指令还用以实现以下步骤：

再次随机显示问题对话框；

当判断再次显示的问题对话框中的待验答案与标准答案之间不匹配时，将所述人脸图像

发送给审核者进行审核；

当接收到所述审核者的审核结果为所述人脸图像对应的人员不具有对所述第二密级文件进行操作权限的人员时，将所述人脸图像移除所述白名单中。

16. 一种非易失性计算机可读存储介质，所述非易失性计算机可读存储介质上存储有至少一个计算机可读指令，其特征在于，所述计算机可读指令被处理器执行以实现以下步骤：

接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像；

当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框；

当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件对应的密码是否匹配；

当确定所述密码与预设的所述第一密级文件对应的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识，所述加密标识用于提示不具有对所述第二密级文件进行操作权限的用户不能对所述第二密级文件进行操作；

接收到对所述第二密级文件的第二操作时，随机弹出问题对话框；

当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配；

当确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。

17. 如权利要求 16 所述的非易失性计算机可读存储介质，其特征在于，所述至少一个计算机可读指令被所述处理器执行以实现显示对应所述人脸图像的密码输入框时，包括：

识别所述人脸图像中的用户对应的角色权限；

当所述角色权限为第一角色权限时，直接对所述第一密级文件进行所述第一操作；

当所述角色权限为第二角色权限时，显示对应所述第二角色权限的密码输入框。

18. 如权利要求 16 所述的非易失性计算机可读存储介质，其特征在于，所述至少一个计算机可读指令被所述处理器执行以实现所述判断所述密码与预设的所述第一密级文件对应的密码是否匹配时，包括：

获取与所述人脸图像对应的所述第一密级文件的目标密码，不同的人脸图形对应所述第一密级文件的目标密码不同；

判断所述密码与所述目标密码是否匹配。

19. 如权利要求 16 所述的非易失性计算机可读存储介质，其特征在于，所述至少一个计

算机可读指令被所述处理器执行以实现随机弹出问题对话框时，包括：

提取所述第二密级文件的文件内容中的多个第一关键词；

根据每个所述第一关键词首次出现的位置顺序确定所述每个第一关键词的编号；

采用随机数生成算法生成一个随机数；

根据所述随机数与编号之间的对应关系筛选出对应所述随机数的第一目标关键词；

弹出与所述第一目标关键词对应的问题对话框，所述问题对话框中显示有与所述第一目标关键词对应的问题。

20. 如权利要求 16 至 19 中任意一项所述的非易失性计算机可读存储介质，其特征在于，所述至少一个计算机可读指令被所述处理器执行以实现所述判断所述待验答案与所述问题的标准答案是否匹配时，包括：

根据预设匹配度计算规则计算所述待验答案与所述标准答案之间的匹配度；

获取所述第二密级文件对应的预设匹配度阈值；

判断所述匹配度是否大于所述匹配度阈值；

当所述匹配度大于或者等于所述匹配度阈值时，确定所述待验答案与所述标准答案匹配；

当所述匹配度小于所述匹配度阈值时，确定所述待验答案与所述标准答案不匹配。

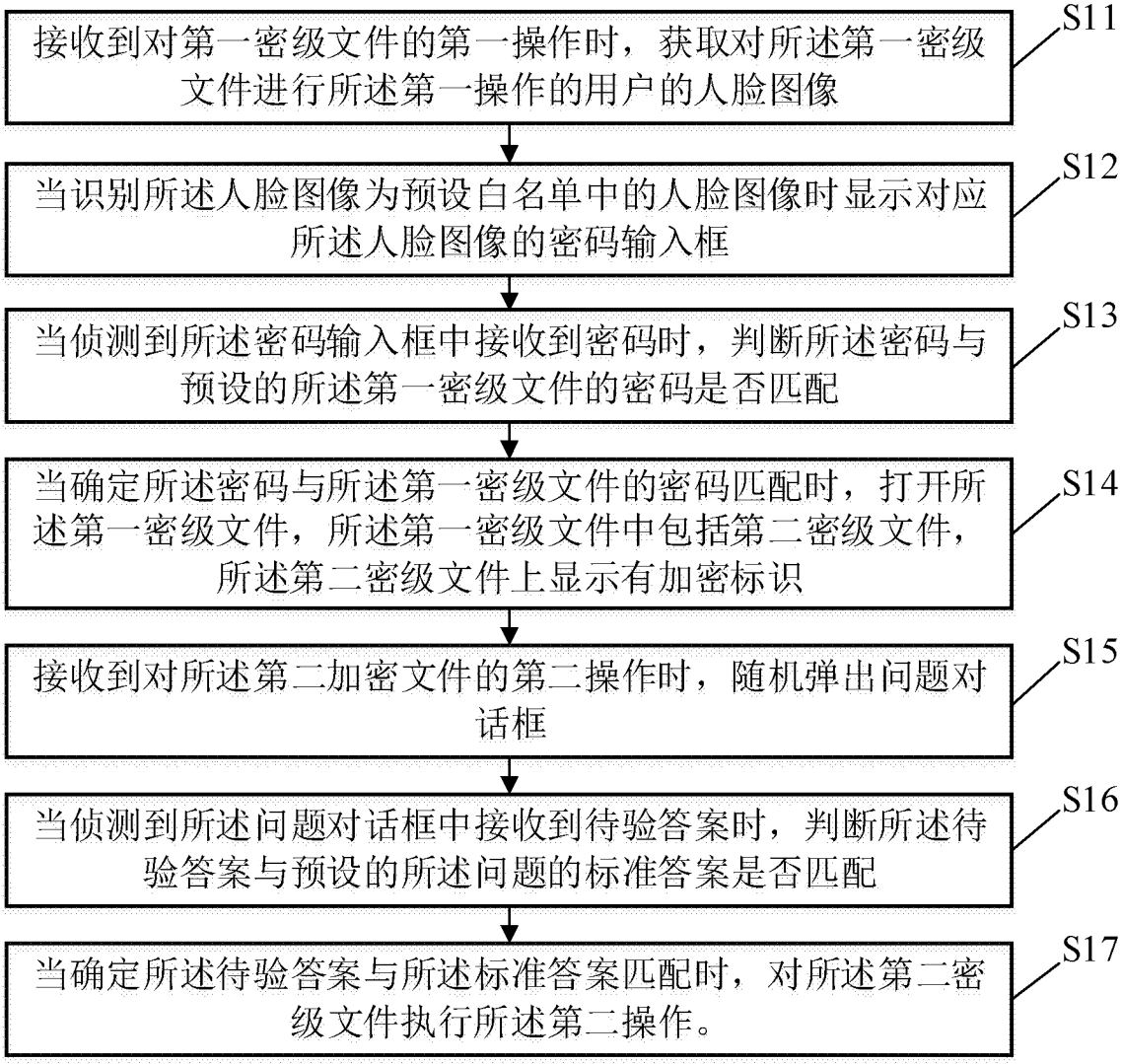
接收到对第一密级文件的第一操作时，获取对所述第一密级文件进行所述第一操作的用户的人脸图像
S11
当识别所述人脸图像为预设白名单中的人脸图像时显示对应所述人脸图像的密码输入框
S12
当侦测到所述密码输入框中接收到密码时，判断所述密码与预设的所述第一密级文件的密码是否匹配
S13
当确定所述密码与所述第一密级文件的密码匹配时，打开所述第一密级文件，所述第一密级文件中包括第二密级文件，所述第二密级文件上显示有加密标识
S14
接收到对所述第二加密文件的第二操作时，随机弹出问题对话框
S15
当侦测到所述问题对话框中接收到待验答案时，判断所述待验答案与预设的所述问题的标准答案是否匹配
S16
当确定所述待验答案与所述标准答案匹配时，对所述第二密级文件执行所述第二操作。
S17

图 1

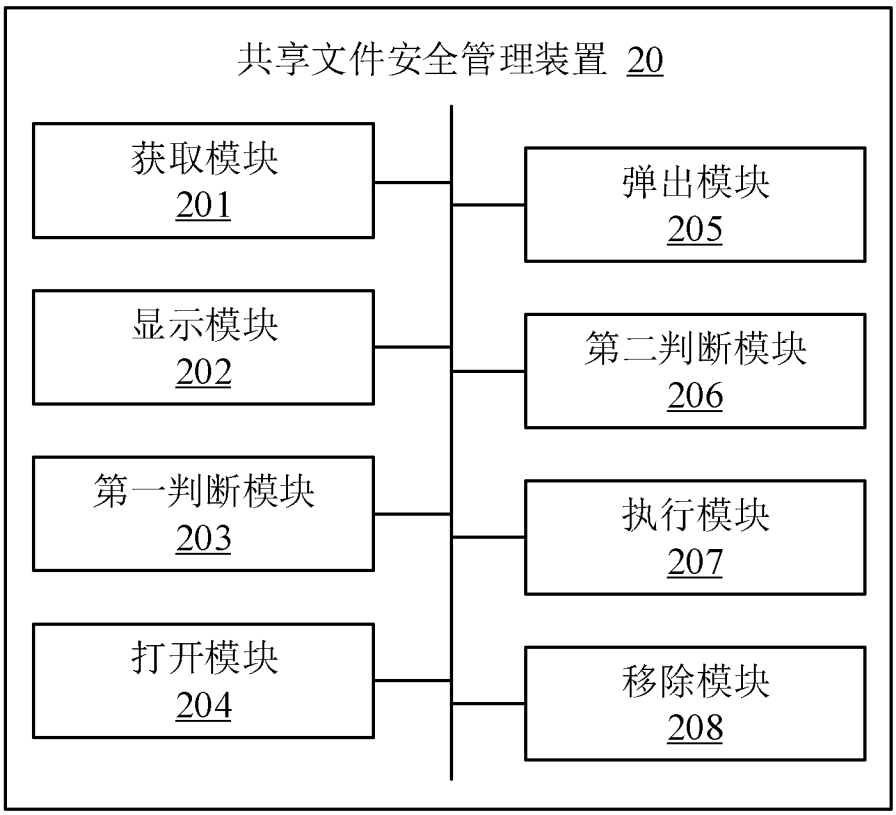
共享文件安全管理装置 20
获取模块
201
显示模块
202
第一判断模块
203
打开模块
204
弹出模块
205
第二判断模块
206
执行模块
207
移除模块
208

图 2

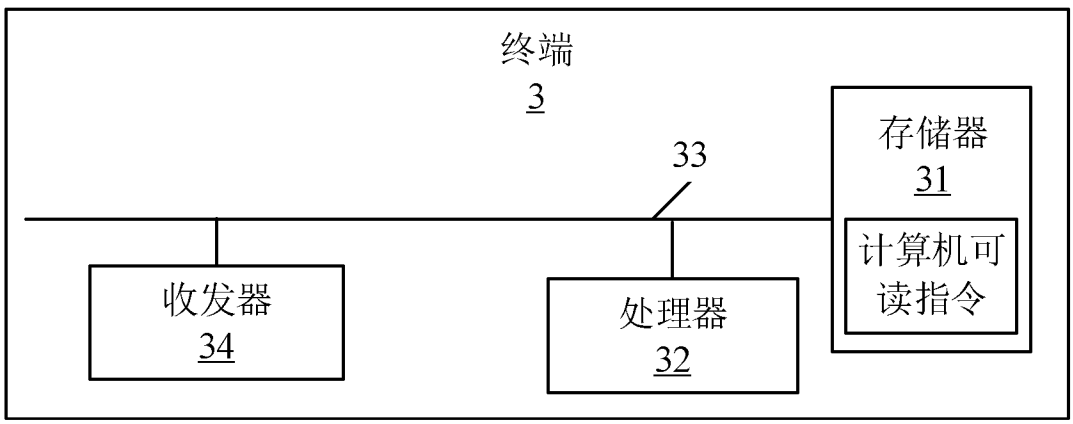
终端
3
33
存储器
31
计算机可读指令
收发器
34
处理器
32

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118599

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i

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)

G06F

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: 文件, 安全, 人脸, 指纹, 生物, 密码, 匹配, 加密, 权限, 问题, 答案, 验证, document, security, face, fingerprint, biological, password, code, match, encryption, authority, question, answer, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110414246 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 05 November 2019 (2019-11-05) description, paragraphs [0006]-[0053]	1-20
Y	CN 109344588 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 15 February 2019 (2019-02-15) description, paragraphs [0035]-[0054]	1-20
Y	CN 105827409 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) 03 August 2016 (2016-08-03) description, paragraphs [0006]-[0024]	1-20
A	CN 106549920 A (HUAWEI TERMINAL (DONGGUAN) CO., LTD.) 29 March 2017 (2017-03-29) entire document	1-20
A	CN 105631272 A (YUNNAN UNIVERSITY) 01 June 2016 (2016-06-01) entire document	1-20
A	CN 107734197 A (HENAN HAODE TECHNOLOGY CO., LTD.) 23 February 2018 (2018-02-23) entire document	1-20

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 February 2020	**18 March 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118599

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016110543 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 21 April 2016 (2016-04-21) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/118599

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110414246 A	05 November 2019	None	
CN 109344588 A	15 February 2019	None	
CN 105827409 A	03 August 2016	None	
CN 106549920 A	29 March 2017	WO 2017050093 A1	30 March 2017
CN 105631272 A	01 June 2016	None	
CN 107734197 A	23 February 2018	None	
US 2016110543 A1	21 April 2016	KR 20160046640 A	29 April 2016

国际检索报告

国际申请号
PCT/CN2019/118599

A. 主题的分类

G06F 21/60(2013.01)i

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)

G06F

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:文件，安全，人脸，指纹，生物，密码，匹配，加密，权限，问题，答案，验证，document，security，face，fingerprint，biological，password，code，match，encryption，authority，question，answer，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
PX	CN 110414246 A (平安科技深圳有限公司) 2019年 11月 5日 (2019-11-05) 说明书第[0006]-[0053]段	1-20
Y	CN 109344588 A (平安科技深圳有限公司) 2019年 2月 15日 (2019-02-15) 说明书第[0035]-[0054]段	1-20
Y	CN 105827409 A (宇龙计算机通信科技深圳有限公司) 2016年 8月 3日 (2016-08-03) 说明书第[0006]-[0024]段	1-20
A	CN 106549920 A (华为终端东莞有限公司) 2017年 3月 29日 (2017-03-29) 全文	1-20
A	CN 105631272 A (云南大学) 2016年 6月 1日 (2016-06-01) 全文	1-20
A	CN 107734197 A (河南浩德科技有限公司) 2018年 2月 23日 (2018-02-23) 全文	1-20
A	US 2016110543 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 2016年 4月 21日 (2016-04-21) 全文	1-20

☐ 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	国际检索报告邮寄日期
2020年 2月 29日	2020年 3月 18日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 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 焦月 电话号码 86-(10)-53961306

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/118599

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 110414246 A	2019年 11月 5日	无	
CN 109344588 A	2019年 2月 15日	无	
CN 105827409 A	2016年 8月 3日	无	
CN 106549920 A	2017年 3月 29日	WO 2017050093 A1	2017年 3月 30日
CN 105631272 A	2016年 6月 1日	无	
CN 107734197 A	2018年 2月 23日	无	
US 2016110543 A1	2016年 4月 21日	KR 20160046640 A	2016年 4月 29日