(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115471937 B
(45)授权公告日 2024.04.19

(21)申请号 202211167327.9

(22)申请日 2022.09.23

(65)同一申请的已公布的文献号
申请公布号 CN 115471937 A

(43)申请公布日 2022.12.13

(73)专利权人 广州浩传网络科技有限公司
地址 510000 广东省广州市天河区元岗路310号自编3栋C213单元

(72)发明人 林铤 马晓亮

(74)专利代理机构 佛山信智汇知识产权代理事务所(特殊普通合伙) 44629
专利代理师 冯桂彬

(51)Int.Cl.
G07C 9/00(2020.01)
G07F 17/12(2006.01)
A47B 63/00(2006.01)

(56)对比文件
CN 110570553 A,2019.12.13
CN 111783059 A,2020.10.16
CN 113763616 A,2021.12.07
CN 114268453 A,2022.04.01
CN 111063067 A,2020.04.24
CN 114697117 A,2022.07.01
CN 103646201 A,2014.03.19
CN 104184589 A,2014.12.03
CN 110415414 A,2019.11.05
CN 112252853 A,2021.01.22
CN 112309525 A,2021.02.02
CN 217061056 U,2022.07.26
WO 2017024550 A1,2017.02.16
WO 2022052780 A1,2022.03.17
王子.信息系统用户身份认证的安全性分析.信息技术与信息化.2017,(第06期),全文.

审查员 黄丹

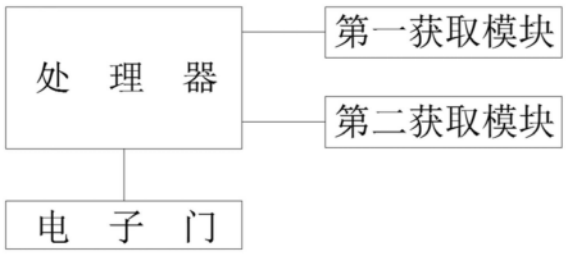
权利要求书2页 说明书8页 附图1页

(54)发明名称

一种档案管理装置及使用方法

(57)摘要

本发明设计档案管理技术领域,提供了一种档案管理装置及使用方法,该档案管理装置包括处理器、柜体、电子门、第一获取模块以及第二获取模块,处理器根据第一验证成功结果以及第二验证成功结果打开或关闭与用户身份信息相对应的电子门,第一获取模块用于获取第一验证信息以及与第一验证信息关联的第二验证信息,根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果,第二获取模块用于获取用户身份信息以及第二验证信息,根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果。本发明可以对用户权限进行多重验证,提高了纸质档案的安全性。



CN 115471937 B

1.一种档案管理装置,包括处理器、具有多个储物位的柜体以及多个电子门,储物位用于存储档案文件,电子门安装在储物位上且与储物位一一对应,其特征在于,所述档案管理装置还包括:

第一获取模块,用于获取第一验证信息以及与第一验证信息关联的第二验证信息,根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果并反馈至处理器;

第二获取模块,用于获取用户身份信息以及第二验证信息,根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果并反馈至处理器;

其中,处理器还用于根据第一验证成功结果以及第二验证成功结果打开与用户身份信息相对应的电子门;

其中,第二获取模块包括摄像单元,所述档案管理装置还包括:

输入模块,与第一获取模块通信连接,用于获取用户输入的第一验证信息并反馈至第一获取模块;

显示模块,用于根据第一验证信息生成并显示第二验证信息;

其中,摄像单元用于拍摄实时区域图像,根据实时区域图像获取用户身份信息以及第二验证信息。

2.如权利要求1所述的一种档案管理装置,其特征在于,第一获取模块包括第一摄像单元,第二获取模块包括第二摄像单元,所述档案管理装置还包括:

输入模块,与第一获取模块通信连接,用于获取用户输入的第一验证信息并反馈至第一获取模块;

显示模块,用于根据第一验证信息生成并显示第二验证信息;

其中,第一摄像单元用于拍摄第一实时区域图像并根据第一实时区域图像获取第二验证信息,第二摄像单元用于获取第二实时区域图像并根据第二实时区域图像获取用户身份信息以及第二验证信息。

3.如权利要求1所述的一种档案管理装置,其特征在于,所述第一验证信息为随机更新的数字验证码,所述第二验证信息为第一验证信息的哈希序列。

4.一种档案管理装置使用方法,其特征在于,所述档案管理装置使用方法包括如下步骤:

S1,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息;

S2,第一获取模块根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果并反馈至处理器;

S3,第二获取模块获取用户身份信息以及第二验证信息;

S4,第二获取模块根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果并反馈至处理器;

S5,处理器根据第一验证成功结果以及第二验证成功结果打开或关闭与用户身份信息相对应的电子门;

其中,在步骤S1中,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息的具体方法包括如下步骤:

提供与第一获取模块通信连接输入模块,通过输入模块获取用户输入的第一验证信息并反馈至第一获取模块;

提供一显示模块,显示模块根据第一验证信息生成并显示第二验证信息;

第一获取模块获取显示模块显示的第二验证信息。

5.如权利要求4所述的一种档案管理装置使用方法,其特征在于,在步骤S3中,第二获取模块获取用户身份信息以及第二验证信息的具体方法包括如下步骤:

通过摄像单元用于拍摄实时区域图像;

第二获取模块根据实时区域图像获取用户身份信息以及第二验证信息。

6.如权利要求4所述的一种档案管理装置使用方法,其特征在于,在步骤S1中,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息的具体方法包括如下步骤:

提供与第一获取模块通信连接输入模块,通过输入模块获取用户输入的第一验证信息并反馈至第一获取模块;

提供一显示模块,显示模块根据第一验证信息生成并显示第二验证信息;

通过第一获取模块的第一摄像单元拍摄第一实时区域图像并根据第一实时区域图像获取第二验证信息;

通过第二获取装置的第二摄像单元获取第二实时区域图像并根据第二实时区域图像获取用户身份信息以及第二验证信息。

7.如权利要求5所述的一种档案管理装置使用方法,其特征在于,所述第一验证信息为随机更新的数字验证码,所述第二验证信息为第一验证信息的哈希序列。

8.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有计算机程序,当所述计算机程序被执行时实现如权利要求4-7任一项所述的档案管理装置使用方法。

一种档案管理装置及使用方法

技术领域

[0001] 本发明涉及档案管理技术领域,具体而言,涉及一种档案管理装置及使用方法。

背景技术

[0002] 档案是人们在社会活动中直接形成的各种具有保存价值的原始记录,在社会化进程中承担着独特的使命。档案包括纸质档案和电子档案。无论纸质档案或者电子档案,都需要进行针对性管理,以保护档案数据的安全,方便用户存储。

[0003] 申请人经过大量检索发现一些典型现有技术,如申请号为202010377290.7的专利公开了一种智能档案柜安全系统,解决了针对拥有不同类型纸质档案的查阅和存取权限的人员进行快速,简单以及智能化的管理以及判断,提高纸质档案的安全性的问题。又如申请号为201610213139.3的专利公开了一种档案管理装置,其通过对档案盒信息记录,通过信息存储器种的信息即可通过指令,利用机械手寻找到目标档案,操作方便、快捷,尤其适合大信息量档案管理。又如申请号为202010104735.4的专利公开了一种档案管理系统,其有效提高了加密的难度,避免外人破解打开档案柜,通过智能化的变化密码以及调整输入密码的输入方式,大大避免了外人登录的可能性。

[0004] 由此可知,对于档案管理在实际应用中亟待处理的许多问题(比如如何提高纸质档案安全性等),还存在许多未提出的技术方案。

发明内容

[0005] 基于此,为了提高纸质档案的安全性,本发明提供了一种档案管理装置及使用方法,其具体技术方案如下:

[0006] 一种档案管理装置,包括处理器、具有多个储物位的柜体以及多个电子门,储物位用于存储档案文件,电子门安装在储物位上且与储物位一一对应;所述档案管理装置还包括第一获取模块以及第二获取模块。

[0007] 第一获取模块用于获取第一验证信息以及与第一验证信息关联的第二验证信息,根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果并反馈至处理器。

[0008] 第二获取模块用于获取用户身份信息以及第二验证信息,根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果并反馈至处理器。

[0009] 其中,处理器还用于根据第一验证成功结果以及第二验证成功结果打开与用户身份信息相对应的电子门。

[0010] 所述档案管理装置通过设置第一获取模块以及第二获取模块,分别利用第一验证信息、第二验证信息以及用户身份信息对用户权限进行验证,其不仅包括通过第一验证信息和第二验证信息对用户权限的单独验证,还包括通过用户身份信息以及第二验证信息对用户权限的联合验证,可以对用户权限进行多重验证,提高了纸质档案的安全性。

[0011] 进一步地,第二获取模块包括摄像单元,所述档案管理装置还包括:

[0012] 输入模块,与第一获取模块通信连接,用于获取用户输入的第一验证信息并反馈至第一获取模块;

[0013] 显示模块,用于根据第一验证信息生成并显示第二验证信息;

[0014] 其中,摄像单元用于拍摄实时区域图像,根据实时区域图像获取用户身份信息以及第二验证信息。

[0015] 进一步地,第一获取模块包括第一摄像单元,第二获取模块包括第二摄像单元,所述档案管理装置还包括:

[0016] 输入模块,与第一获取模块通信连接,用于获取用户输入的第一验证信息并反馈至第一获取模块;

[0017] 显示模块,用于根据第一验证信息生成并显示第二验证信息;

[0018] 其中,第一摄像单元用于拍摄第一实时区域图像并根据第一实时区域图像获取第二验证信息,第二摄像单元用于获取第二实时区域图像并根据第二实时区域图像获取用户身份信息以及第二验证信息。

[0019] 进一步地,所述第一验证信息为随机更新的数字验证码,所述第二验证信息为第一验证信息的哈希序列。

[0020] 一种档案管理装置使用方法,其包括如下步骤:

[0021] S1,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息;

[0022] S2,第一获取模块根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果并反馈至处理器;

[0023] S3,第二获取模块获取用户身份信息以及第二验证信息;

[0024] S4,第二获取模块根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果并反馈至处理器;

[0025] S5,处理器根据第一验证成功结果以及第二验证成功结果打开或关闭与用户身份信息相对应的电子门。

[0026] 进一步地,在步骤S1中,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息的具体方法包括如下步骤:

[0027] 提供与第一获取模块通信连接输入模块,通过输入模块获取用户输入的第一验证信息并反馈至第一获取模块;

[0028] 提供一显示模块,显示模块根据第一验证信息生成并显示第二验证信息;

[0029] 第一获取模块获取显示模块显示的第二验证信息。

[0030] 进一步地,在步骤S3中,第二获取模块获取用户身份信息以及第二验证信息的具体方法包括如下步骤:

[0031] 通过摄像单元用于拍摄实时区域图像;

[0032] 第二获取模块根据实时区域图像获取用户身份信息以及第二验证信息。

[0033] 进一步地,在步骤S1中,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息的具体方法包括如下步骤:

[0034] 提供与第一获取模块通信连接输入模块,通过输入模块获取用户输入的第一验证信息并反馈至第一获取模块;

[0035] 提供一显示模块,显示模块根据第一验证信息生成并显示第二验证信息;

[0036] 通过第一获取模块的第一摄像单元拍摄第一实时区域图像并根据第一实时区域图像获取第二验证信息;

[0037] 通过第二获取装置的第二摄像单元获取第二实时区域图像并根据第二实时区域图像获取用户身份信息以及第二验证信息。

[0038] 进一步地,所述第一验证信息为随机更新的数字验证码,所述第二验证信息为第一验证信息的哈希序列。

[0039] 进一步地,一种计算机可读存储介质,其存储有计算机程序,当所述计算机程序被执行时实现所述的档案管理装置使用方法。

附图说明

[0040] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制,而是将重点放在示出实施例的原理上。在不同的视图中,相同的附图标记指定对应的部分。

[0041] 图1是本发明一实施例中一种档案管理装置的整体结构示意图一;

[0042] 图2是本发明一实施例中一种档案管理装置的整体结构示意图二。

[0043] 附图标记说明:

[0044] 1、输入模块;2、显示模块;3、摄像单元。

具体实施方式

[0045] 为了使得本发明的目的、技术方案及优点更加清楚明白,以下结合其实施例,对本发明进行进一步详细说明。应当理解的是,此处所描述的具体实施方式仅用以解释本发明,并不限定本发明的保护范围。

[0046] 需要说明的是,当元件被称为“固定于”另一个元件,它可以直接在另一个元件上或者也可以存在居中的元件。当一个元件被认为是“连接”另一个元件,它可以是直接连接到另一个元件或者可能同时存在居中元件。本文所使用的术语“垂直的”、“水平的”、“左”、“右”以及类似的表述只是为了说明的目的,并不表示是唯一的实施方式。

[0047] 除非另有定义,本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文中在本发明的说明书中所使用的术语只是为了描述具体的实施方式的目的,不是旨在于限制本发明。本文所使用的术语“及/或”包括一个或多个相关的所列项目的任意的和所有的组合。

[0048] 本发明中所述“第一”、“第二”不代表具体的数量及顺序,仅仅是用于名称的区分。

[0049] 如图1所示,本发明一实施例中的一种档案管理装置,包括处理器、具有多个储物位的柜体以及多个电子门,储物位用于存储档案文件,电子门安装在储物位上且与储物位一一对应;所述档案管理装置还包括第一获取模块以及第二获取模块。

[0050] 第一获取模块用于获取第一验证信息以及与第一验证信息关联的第二验证信息,根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果并反馈至处理器。

[0051] 第二获取模块用于获取用户身份信息以及第二验证信息,根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果并反

馈至处理器。

[0052] 其中,处理器还用于根据第一验证成功结果以及第二验证成功结果打开与用户身份信息相对应的电子门。每一个用户分配一个唯一的储物位。打开电子门后,用户即可以进行纸质档案存取操作。

[0053] 电子门包括门体以及电子锁,门体铰接在储物位上,电子锁与处理器通信连接或电连接。由于电子门属于现有技术,在此不再赘述。

[0054] 具体而言,所述第一验证信息包括但不限于随机更新的数字验证码,所述第二验证信息为第一验证信息的哈希序列。

[0055] 数字验证码可以通过短信方式,发送至需要存取纸质档案的用户。优选地,可以将数字验证码发送至与用户个人身份绑定的移动终端或可佩戴设备。

[0056] 第一验证信息为随机更新的数字验证码的目的在于,可以随机且动态地更新第一验证信息,提高用户权限验证的可靠性。

[0057] 第一验证信息通过哈希函数转换后所得到对应的哈希序列,作为第二验证信息,使得第一验证信息与第二验证信息彼此关联。

[0058] 第一验证信息可以由处理器生成并发送至移动终端又或者可佩戴设备,用户通过移动终端或可佩戴设备获取第一验证信息并反馈至第一获取装置。

[0059] 第一获取装置在获取到第一验证信息以及第二验证信息后,根据第一验证信息以及第二验证信息对用户权限进行验证,若第一验证信息与第二验证信息匹配一致,则用户权限通过验证,生成第一验证成功结果并反馈至处理器。

[0060] 当然,处理器生成的第一验证信息也可以是数字标签又或者图像标签并发送至用户移动终端,用户通过移动终端对第一验证信息进行显示。第一获取装置扫描并获取用户移动终端所显示的第一验证信息。在这里,第二验证信息则可以是第一验证信息经过数字转码以及哈希变换后的哈希序列。

[0061] 第二验证信息通过显示模块进行显示,并且显示模块配置成可被第一获取装置以及第二获取装置获取。设置第二验证信息的目的在于,第一获取装置可以通过获取并验证第一验证信息与第二验证信息是否匹配一致,来验证用户权限。与此同时,第二获取装置通过获取柜体预设半径范围内实时区域图像,提取实时区域图像中的用户人脸图像以及第二验证信息,可以对用户身份信息以及第二验证信息进行联合验证。

[0062] 由于移动终端或者可佩戴设备与用户个人身份绑定,故而第一获取装置通过获取第二验证信息以及移动终端或可佩戴设备反馈的第一验证信息,可以利用第一验证信息和第二验证信息对用户权限进行单独验证。即是说,当第一验证信息以及第二验证信息匹配一致且移动终端或可佩戴设备反馈的第一验证信息与处理器生成的第一验证信息匹配一致,则用户权限通过验证并生成第一验证成功结果。

[0063] 第二获取模块用于获取用户身份信息以及第二验证信息,根据用户身份信息以及第二验证信息对用户权限进行联合验证。在这里,用户身份信息为用户人脸图像。

[0064] 联合验证的意思是:第二获取模块通过获取柜体预设半径范围内实时区域图像,提取实时区域图像中的用户人脸图像以及第二验证信息,若用户人脸图像以及第二验证信息均在同一张实时区域图像并且用户人脸图像以及第二验证信息分别与预存的用户人脸图像以及第一验证信息相匹配,则用户权限通过验证,若用户权限通过验证,则生成第二验

证成功结果并反馈至处理器。

[0065] 所述档案管理装置通过设置第一获取模块以及第二获取模块,分别利用第一验证信息、第二验证信息以及用户身份信息对用户权限进行验证,其不仅包括通过第一验证信息和第二验证信息对用户权限的单独验证,还包括通过用户身份信息以及第二验证信息对用户权限的联合验证,可以对用户权限进行多重验证,提高了纸质档案的安全性。

[0066] 在其中一个实施例中,第二获取模块包括摄像单元,所述档案管理装置还包括输入模块以及显示模块。

[0067] 输入模块与第一获取模块通信连接,用于获取用户输入的第一验证信息并反馈至第一获取模块。

[0068] 处理器在将第一验证信息发送至移动终端或可佩戴设备后,用户通过输入模块将第一验证信息反馈至第一获取模块。由于移动终端和可佩戴设备均与用户个人身份绑定,故而当第一获取装置获取到的第二验证信息与用户输入的第一验证信息匹配一致,则可以判定用户权限通过验证。

[0069] 显示模块用于根据第一验证信息生成并显示第二验证信息。其中,摄像单元用于拍摄实时区域图像,根据实时区域图像获取用户身份信息以及第二验证信息。

[0070] 第二获取模块提取摄像单元拍摄的实时区域图像中的用户身份信息以及第二验证信息,若用户身份信息与第二验证信息均处在同一张实时区域图像并且用户身份信息以及第二验证信息分别与预存的用户身份信息像以及第一验证信息相匹配时,则可以判定用户权限通过验证并生成第二验证成功结果。

[0071] 在这里,用户身份信息可以为用户人脸图像。显示模块与第一获取模块通信连接,并将生成的第二验证信息反馈至第一获取模块。

[0072] 显示模块被配置成可配第二获取模块的摄像单元拍摄到,并且第二获取模块的摄像单元被配置成可同时拍摄到显示模块以及用户人脸图像。比如,如图2所示,输入模块1安装在柜体的一侧,显示模块2安装在柜体的另一侧,第二获取模块的摄像单元3安装在输入模块的顶部。即是说,显示模块与输入模块相对设置,用户在通过输入模块输入第一验证信息时,第二获取模块的摄像单元能够拍摄到包括用户人脸图像以及显示模块的实时区域图像。第二获取模块的摄像单元3优选为广角摄像头或者半球摄像头,以便能够同时捕捉到显示模块以及用户人脸图像区域。

[0073] 通过设置输入模块,可以方便第一获取模块获取用户输入的第一验证信息。设置显示模块以及摄像单元,通过识别实时区域图像中的用户人脸图像以及第二验证信息,可以对用户权限进行验证。

[0074] 在其中一个实施例中,第一获取模块包括第一摄像单元,第二获取模块包括第二摄像单元,所述档案管理装置还包括输入模块以及显示模块。

[0075] 输入模块与第一获取模块通信连接,用于获取用户输入的第一验证信息并反馈至第一获取模块。处理器在将第一验证信息发送至移动终端或可佩戴设备后,用户通过输入模块将第一验证信息反馈至第一获取模块。

[0076] 显示模块用于根据第一验证信息生成并显示第二验证信息。

[0077] 其中,第一摄像单元用于拍摄第一实时区域图像并根据第一实时区域图像获取第二验证信息,第二摄像单元用于获取第二实时区域图像并根据第二实时区域图像获取用户

身份信息以及第二验证信息。

[0078] 在这里,第二验证信息通过显示模块进行显示,第一获取模块通过第一摄像单元拍摄的第一实时区域图像获取第二验证信息。

[0079] 通过设置输入模块、显示模块以及第一摄像单元,可以方便第一获取模块获取第一验证信息以及第二验证信息。通过设置显示模块以及第二摄像单元,可以方便第二获取模块获取用户身份信息以及第二验证信息。

[0080] 作为一种优选的技术方案,第一验证信息还可以是图像标签比如二维码标签,处理器生成图像标签并发送至移动终端。移动终端显示图像标签并被第一摄像单元捕捉拍摄。

[0081] 即是说,第一获取模块包括第一摄像单元,第二验证信息通过显示模块显示出来,显示模块相对摄像单元安装设置并且显示模块显示的第二验证信息可被摄像单元捕捉拍摄到。

[0082] 用户通过移动终端显示图像标签并将移动终端屏幕对准摄像单元,无需手动输入第一验证信息。如此一来,通过第一获取模块的第一摄像单元获取第一实时区域图像,即可以提取到第一实时区域图像中的第一验证信息以及第二验证信息。若第一实时区域图像中的第一验证信息以及第二验证信息匹配一致,则用户权限通过验证,生成第一验证成功结果并反馈至处理器。

[0083] 第二获取模块包括第二摄像单元,第二摄像单元用来拍摄第二实时区域图像,第二获取模块通过提取第二实时区域图像中的用户身份信息以及第二验证信息,即可以对用户权限进行验证;若用户权限验证通过,则生成第二验证成功结果并反馈至处理器。

[0084] 第一实时区域图像中包括第一验证信息以及第二验证信息并且第一验证信息与第二验证信息匹配一致,表示与用户个人身份绑定的移动终端处于柜体的预设半径范围内并且用户通过移动终端反馈的第一验证信息准确无误。

[0085] 在这里,第一获取装置通过第一实时区域图像中的第一验证信息以及第二验证信息对用户权限进行验证,其不仅包括通过第一验证信息和第二验证信息对用户权限的单独验证,实际上还包括通过对与用户个人身份绑定的移动终端实际位置对用户权限的验证。

[0086] 综上所述,通过设置第一摄像单元以及第二摄像单元,所述档案管理装置可以利用第一实时区域图像中的第一验证信息以及第二验证信息、与用户个人身份绑定的移动终端实际位置、第二实时区域图像中的用户身份信息以及第二验证信息对用户权限进行多重验证,提高了纸质档案的安全性。

[0087] 在其中一个实施例中,一种档案管理装置使用方法,其包括如下步骤:

[0088] S1,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息。

[0089] S2,第一获取模块根据第一验证信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第一验证成功结果并反馈至处理器。

[0090] S3,第二获取模块获取用户身份信息以及第二验证信息。

[0091] S4,第二获取模块根据用户身份信息以及第二验证信息对用户权限进行验证,若用户权限通过验证,则生成第二验证成功结果并反馈至处理器。

[0092] S5,处理器根据第一验证成功结果以及第二验证成功结果打开或关闭与用户身份信息相对应的电子门。

[0093] 具体而言,在步骤S1中,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息的具体方法包括如下步骤:

[0094] S10,提供与第一获取模块通信连接输入模块,通过输入模块获取用户输入的第一验证信息并反馈至第一获取模块;

[0095] S11,提供一显示模块,显示模块根据第一验证信息生成并显示第二验证信息。

[0096] S12,第一获取模块获取显示模块显示的第二验证信息。

[0097] 在步骤S3中,第二获取模块获取用户身份信息以及第二验证信息的具体方法包括如下步骤:

[0098] S30,通过摄像单元用于拍摄实时区域图像;

[0099] S31,第二获取模块根据实时区域图像获取用户身份信息以及第二验证信息。

[0100] 其中,所述第一验证信息为随机更新的数字验证码,所述第二验证信息为第一验证信息的哈希序列。

[0101] 所述档案管理装置使用方法通过设置第一获取模块以及第二获取模块,分别利用第一验证信息、第二验证信息以及用户身份信息对用户权限进行验证,其不仅包括通过第一验证信息和第二验证信息对用户权限的单独验证,还包括通过用户身份信息以及第二验证信息对用户权限的联合验证,可以对用户权限进行多重验证,提高了纸质档案的安全性。

[0102] 在其中一个实施例中,在步骤S1中,第一获取模块获取第一验证信息以及与第一验证信息关联的第二验证信息的具体方法包括如下步骤:

[0103] 提供与第一获取模块通信连接输入模块,通过输入模块获取用户输入的第一验证信息并反馈至第一获取模块;

[0104] 提供一显示模块,显示模块根据第一验证信息生成并显示第二验证信息;

[0105] 通过第一获取模块的第一摄像单元拍摄第一实时区域图像并根据第一实时区域图像获取第二验证信息;

[0106] 通过第二获取装置的第二摄像单元获取第二实时区域图像并根据第二实时区域图像获取用户身份信息以及第二验证信息。

[0107] 通过设置输入模块、显示模块以及第一摄像单元,可以方便第一获取模块获取第一验证信息以及第二验证信息。通过设置显示模块以及第二摄像单元,可以方便第二获取模块获取用户身份信息以及第二验证信息。

[0108] 在其中一个实施例中,处理器在向移动终端发送第一验证信息前,向移动终端发送坐标获取请求,移动终端根据坐标获取请求向处理器发送自身定位坐标,处理器根据移动终端的自身定位坐标生成第一验证信息并反馈至移动终端。具体而言,移动终端利用自身定位模块获取定位坐标数值,处理器利用预设算法(比如哈希函数)将定位坐标转换成第一验证信息。

[0109] 在移动终端上,设置有相应小程序或者虚拟按钮。用户通过小程序或者虚拟按钮生成档案获取请求并发送至处理器,处理器根据档案获取请求,生成坐标获取请求。

[0110] 如此一来,第一验证信息与移动终端的定位坐标直接相关,第二验证信息与移动终端的定位坐标间接相关。处理器通过移动终端的定位坐标获取第一验证信息,可以更好地对用户权限进行验证,保证用户权限验证的准确无误。由于在用户前往档案室存取纸质档案室,移动终端的定位坐标往往处在不断变化当中,故而利用移动终端的定位坐标获取

第一验证信息,可以保证第一验证信息的随机更新,提高了第一验证信息以及纸质档案存取的安全性。

[0111] 作为一种优选的技术方案,第一验证信息为随机更新的数字验证码且随机更新的方法包括如下步骤:

[0112] 第一步,在储物位内安装一个与处理器信号连接的密码锁,处理器获取密码锁的密码并作为密码种子数字;所述密码锁被配置成可根据用户操作而改变密码种子数字。具体而言,密码锁是拨轮式电子密码锁,用户通过拨动拨轮,改变密码种子数字。

[0113] 密码锁采用拨轮式电子密码锁的作用,在于可以在电子门关闭后,保持用户所设置的密码种子数字,方便处理器获取用户最终设置的密码种子数字。

[0114] 第二步,处理器获取储物位电子门完成纸质档案存取后(即电子门处在关闭状态时)的密码锁的密码种子数字,并向移动终端发送坐标获取请求,移动终端根据坐标获取请求向处理器发送自身定位坐标,处理器根据移动终端反馈的自身定位坐标以及密码种子数字生成第一验证信息并反馈至移动终端。

[0115] 具体而言,移动终端利用自身定位模块获取定位坐标数值,处理器利用预设算法(比如哈希函数)将定位坐标以及密码种子数字转换成第一验证信息。比如说,可以将定位坐标与密码种子数字进行拼接、异或又或者同或后,在通过预设算法转换成第一验证信息。

[0116] 如此一来,通过将密码锁安装在储物位中,用户在设置密码种子数字时,不容易被旁边的人看到密码种子数字,保证了密码种子数字的安全。在此基础上,利用密码种子数字以及移动终端的定位坐标,即便用户移动终端发送至处理器的定位坐标被他人获取,他人也无法根据定位坐标以及预设算法获取正确的第一验证信息,进一步提高了纸质档案存取的安全性。

[0117] 在其中一个实施例中,一种计算机可读存储介质,其存储有计算机程序,当所述计算机程序被执行时实现所述的档案管理装置使用方法。

[0118] 以上所述实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0119] 以上所述实施例仅表达了本发明的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变形和改进,这些都属于本发明的保护范围。因此,本发明专利的保护范围应以所附权利要求为准。

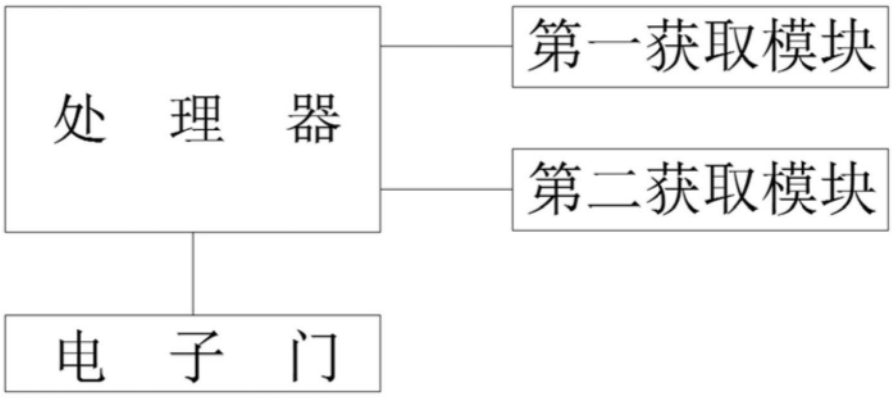


图1

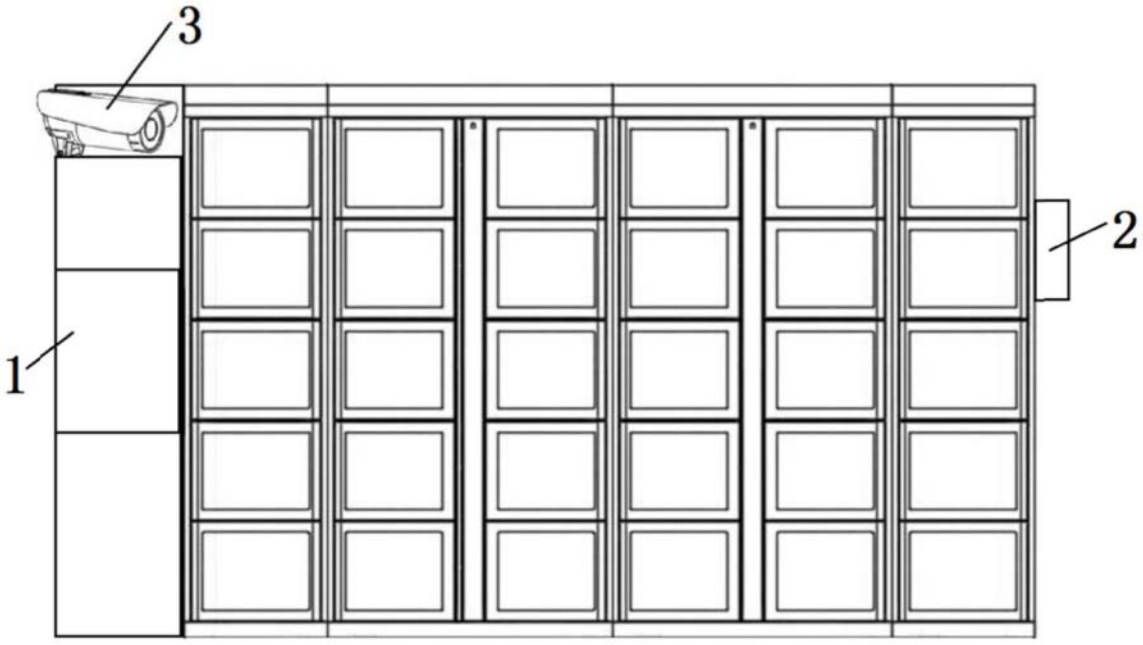


图2