(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116680673 B
(45)授权公告日 2024.04.16

(21)申请号 202310732768.7

(22)申请日 2023.06.20

(65)同一申请的已公布的文献号
申请公布号 CN 116680673 A

(43)申请公布日 2023.09.01

(73)专利权人 深圳市彤兴电子有限公司
地址 518000 广东省深圳市南山区学苑大道1001号南山智园B1栋11层

(72)发明人 刘建华

(74)专利代理机构 深圳汉林汇融知识产权代理事务所(普通合伙) 44850
专利代理师 刘临利

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/60(2013.01)

(56)对比文件
JP 2008042590 A,2008.02.21
KR 20160139885 A,2016.12.07
US 2006072745 A1,2006.04.06
US 2014223580 A1,2014.08.07
WO 2017201896 A1,2017.11.30
WO 2021017128 A1,2021.02.04
罗维.云存储数据安全与共享方案研究.信息科技.2020,(第2期),20-30.
S.G. Stubblebine.On messsage integrity in cryptographic protocols.Proceeding 1992 IEEE Computer Society Symposium on Research in Security and Privacy.1992,85-104.

审查员 刘佳菡

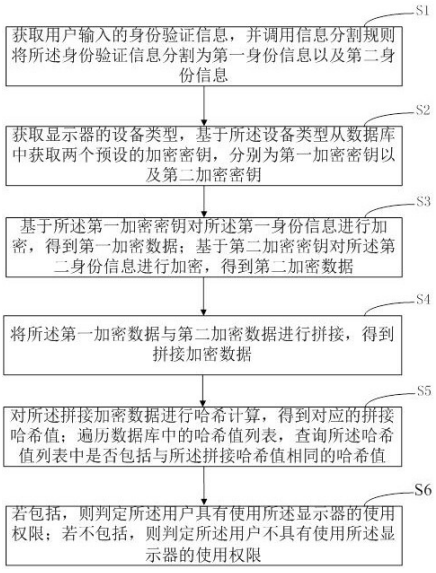
权利要求书3页 说明书10页 附图3页

(54)发明名称

显示器的身份校验方法、装置以及计算机设备

(57)摘要

本发明提供一种显示器的身份校验方法、装置、计算机设备和存储介质,包括:将身份验证信息分割为第一身份信息以及第二身份信息;基于第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;若包括,则判定所述用户具有使用所述显示器的使用权限。本发明中,结合了加密和哈希算法,有效地保护用户的隐私和安全,同时提高身份验证的效率和准确性。



CN 116680673 B

1.一种显示器的身份校验方法,其特征在于,包括以下步骤:

获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;

获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;

基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;

将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;

对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;

若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。

2.根据权利要求1所述的显示器的身份校验方法,其特征在于,所述判定所述用户具有使用所述显示器的使用权限的步骤之后,包括:

生成一个二维码,并将所述第一身份信息以及第二身份信息添加在所述二维码中;

将所述二维码发送至所述用户所持的智能终端上;其中,所述用户在下一次使用所述显示器时,只需要出示所述二维码,无需再次输入身份验证信息。

3.根据权利要求2所述的显示器的身份校验方法,其特征在于,所述生成一个二维码,并将所述第一身份信息以及第二身份信息添加在所述二维码中的步骤,包括:

导入QR Code生成库;

获取所述第一身份信息以及第二身份信息的数据类型,并根据所述数据类型,选择对应的纠错级别;其中,数据库存储有数据类型与纠错级别的映射关系;

获取所述第一身份信息以及第二身份信息的总数据量,获取所述显示器前方的空间距离;根据所述总数据量以及所述空间距离,确定二维码的尺寸和版本;

基于QR Code生成库以及所述纠错级别,将所述第一身份信息以及第二身份信息编码成对应尺寸以及版本的二维码矩阵;

对所述二维码矩阵进行错误校验并生成最终的二维码,将生成的二维码保存为图像文件。

4.根据权利要求1所述的显示器的身份校验方法,其特征在于,所述获取用户输入的身份验证信息的步骤,包括:

接收用户所持终端依序发送的多个数据包,多个数据包按照发送顺序组成数据包序列;

对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括空白数据包;

若包括空白数据包,则检测出包括空白数据包的数据包数量为x,作为第一数量;

从所述数据包序列中,检测出排列在第x位上的目标数据包;

对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息。

5.根据权利要求4所述的显示器的身份校验方法,其特征在于,所述对所述目标数据包

进行解析,获取所述目标数据包中携带的身份验证信息的步骤,包括:

对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括指定的干扰数据包;其中,所述干扰数据包是各个数据包中未加密且携带有数据的数据包;

若包括干扰数据包,则检测出干扰数据包的数据包数量,作为第二数量;

基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为解密密码对所述目标数据包进行解密,得到所述目标数据包中携带的身份验证信息;其中,所述数据包序列中只有所述目标数据包为加密数据。

6.根据权利要求4所述的显示器的身份校验方法,其特征在于,所述用户所持终端依序发送的多个数据包,包括:

所述用户所持终端接收用户输入的所述身份验证信息;

将所述身份验证信息添加至一个数据包中,得到身份数据包;

随机生成第二数量的干扰身份信息,并将所述干扰身份信息添加在数据包中,得到第二数量的干扰数据包;

生成第一数量的空白数据包;

将所有所述干扰数据包与所述空白数据包随机进行排序,得到第一数据包序列;

基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为加密密码对所述身份数据包进行加密,得到目标数据包;

将所述目标数据包插入至所述第一数据包序列中,并使得所述目标数据包位于第x位上,得到第二数据包序列;

基于所述第二数据包序列,依次发送各个数据包至显示器。

7.一种显示器的身份校验装置,其特征在于,包括:

第一获取单元,用于获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;

第二获取单元,用于获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;

加密单元,用于基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;

拼接单元,用于将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;

计算单元,用于对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;

判定单元,用于若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。

8.根据权利要求7所述的显示器的身份校验装置,其特征在于,所述第一获取单元,包括:

接收子单元,用于接收用户所持终端依序发送的多个数据包,多个数据包按照发送顺序组成数据包序列;

第一检测子单元,用于对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括空白数据包;

第二检测子单元,用于若包括空白数据包,则检测出包括空白数据包的数据包数量为x,作为第一数量;

第三检测子单元,用于从所述数据包序列中,检测出排列在第x位上的目标数据包;

解析子单元,用于对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息。

9.根据权利要求8所述的显示器的身份校验装置,其特征在于,所述用户所持终端依序发送的多个数据包,包括:

所述用户所持终端接收用户输入的所述身份验证信息;

将所述身份验证信息添加至一个数据包中,得到身份数据包;

随机生成第二数量的干扰身份信息,并将所述干扰身份信息添加在数据包中,得到第二数量的干扰数据包;

生成第一数量的空白数据包;

将所有所述干扰数据包与所述空白数据包随机进行排序,得到第一数据包序列;

基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为加密密码对所述身份数据包进行加密,得到目标数据包;

将所述目标数据包插入至所述第一数据包序列中,并使得所述目标数据包位于第x位上,得到第二数据包序列;

基于所述第二数据包序列,依次发送各个数据包至显示器。

10.一种计算机设备,包括存储器和处理器,所述存储器中存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1至6中任一项所述方法的步骤。

显示器的身份校验方法、装置以及计算机设备

技术领域

[0001] 本发明涉及数据处理技术领域,特别涉及一种显示器的身份校验方法、装置、计算机设备和存储介质。

背景技术

[0002] 随着数字技术的快速发展,越来越多的设备使用数字环境与处理信息。特别地,显示器作为我们与外部世界进行交流沟通的接口,其安全性和隐私保护也越来越重要。在这个背景下,我们需要开发一种显示器的身份校验方法,以确保仅有授权用户才能使用显示器。

[0003] 而目前,通常没有对显示器的使用权限进行验证,这便使得显示器在数据传输时造成一定的安全风险。

发明内容

[0004] 本发明的主要目的为提供一种显示器的身份校验方法、装置、计算机设备和存储介质。

[0005] 为实现上述目的,本发明提供了一种显示器的身份校验方法,包括以下步骤:

[0006] 获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;

[0007] 获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;

[0008] 基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;

[0009] 将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;

[0010] 对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;

[0011] 若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。

[0012] 进一步地,所述判定所述用户具有使用所述显示器的使用权限的步骤之后,包括:

[0013] 生成一个二维码,并将所述第一身份信息以及第二身份信息添加在所述二维码中;

[0014] 将所述二维码发送至所述用户所持的智能终端上;其中,所述用户在下一次使用所述显示器时,只需要出示所述二维码,无需再次输入身份验证信息。

[0015] 进一步地,所述生成一个二维码,并将所述第一身份信息以及第二身份信息添加在所述二维码中的步骤,包括:

[0016] 导入QR Code生成库;

[0017] 获取所述第一身份信息以及第二身份信息的数据类型,并根据所述数据类型,选择对应的纠错级别;其中,数据库存储有数据类型与纠错级别的映射关系;

[0018] 获取所述第一身份信息以及第二身份信息的总数据量,获取所述显示器前方的空间距离;根据所述总数据量以及所述空间距离,确定二维码的尺寸和版本;

[0019] 基于QR Code生成库以及所述纠错级别,将所述第一身份信息以及第二身份信息编码成对应尺寸以及版本的二维码矩阵;

[0020] 对所述二维码矩阵进行错误校验并生成最终的二维码,将生成的二维码保存为图像文件。

[0021] 进一步地,所述获取用户输入的身份验证信息的步骤,包括:

[0022] 接收用户所持终端依序发送的多个数据包,多个数据包按照发送顺序组成数据包序列;

[0023] 对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括空白数据包;

[0024] 若包括空白数据包,则检测出包括空白数据包的数据包数量为x,作为第一数量;

[0025] 从所述数据包序列中,检测出排列在第x位上的目标数据包;

[0026] 对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息。

[0027] 进一步地,所述对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息的步骤,包括:

[0028] 对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括指定的干扰数据包;其中,所述干扰数据包是各个数据包中未加密且携带有数据的数据包;

[0029] 若包括干扰数据包,则检测出干扰数据包的数据包数量,作为第二数量;

[0030] 基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

[0031] 将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为解密密码对所述目标数据包进行解密,得到所述目标数据包中携带的身份验证信息;其中,所述数据包序列中只有所述目标数据包为加密数据。

[0032] 进一步地,所述用户所持终端依序发送的多个数据包,包括:

[0033] 所述用户所持终端接收用户输入的所述身份验证信息;

[0034] 将所述身份验证信息添加至一个数据包中,得到身份数据包;

[0035] 随机生成第二数量的干扰身份信息,并将所述干扰身份信息添加在数据包中,得到第二数量的干扰数据包;

[0036] 生成第一数量的空白数据包;

[0037] 将所有所述干扰数据包与所述空白数据包随机进行排序,得到第一数据包序列;

[0038] 基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

[0039] 将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为加密密码对所述身份数据包进行加密,得到目标数据包;

[0040] 将所述目标数据包插入至所述第一数据包序列中,并使得所述目标数据包位于第x位上,得到第二数据包序列;

[0041] 基于所述第二数据包序列,依次发送各个数据包至显示器。

[0042] 本发明还提供了一种显示器的身份校验装置,包括:

[0043] 第一获取单元,用于获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;

[0044] 第二获取单元,用于获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;

[0045] 加密单元,用于基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;

[0046] 拼接单元,用于将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;

[0047] 计算单元,用于对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;

[0048] 判定单元,用于若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。

[0049] 进一步地,所述第一获取单元,包括:

[0050] 接收子单元,用于接收用户所持终端依序发送的多个数据包,多个数据包按照发送顺序组成数据包序列;

[0051] 第一检测子单元,用于对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括空白数据包;

[0052] 第二检测子单元,用于若包括空白数据包,则检测出包括空白数据包的数据包数量为x,作为第一数量;

[0053] 第三检测子单元,用于从所述数据包序列中,检测出排列在第x位上的目标数据包;

[0054] 解析子单元,用于对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息。

[0055] 进一步地,所述用户所持终端依序发送的多个数据包,包括:

[0056] 所述用户所持终端接收用户输入的所述身份验证信息;

[0057] 将所述身份验证信息添加至一个数据包中,得到身份数据包;

[0058] 随机生成第二数量的干扰身份信息,并将所述干扰身份信息添加在数据包中,得到第二数量的干扰数据包;

[0059] 生成第一数量的空白数据包;

[0060] 将所有所述干扰数据包与所述空白数据包随机进行排序,得到第一数据包序列;

[0061] 基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

[0062] 将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为加密密码对所述身份数据包进行加密,得到目标数据包;

[0063] 将所述目标数据包插入至所述第一数据包序列中,并使得所述目标数据包位于第

x位上,得到第二数据包序列;

[0064] 基于所述第二数据包序列,依次发送各个数据包至显示器。

[0065] 本发明还提供一种计算机设备,包括存储器和处理器,所述存储器中存储有计算机程序,所述处理器执行所述计算机程序时实现上述任一项所述方法的步骤。

[0066] 本发明还提供一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被处理器执行时实现上述任一项所述的方法的步骤。

[0067] 本发明提供的显示器的身份校验方法、装置、计算机设备和存储介质,包括:获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。本发明中,结合了加密和哈希算法,有效地保护用户的隐私和安全,同时快速、准确地处理用户提交的身份验证信息,提高身份验证的效率和准确性。

附图说明

[0068] 图1是本发明一实施例中显示器的身份校验方法步骤示意图;

[0069] 图2是本发明一实施例中显示器的身份校验装置结构框图;

[0070] 图3是本发明一实施例的计算机设备的结构示意框图。

[0071] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

具体实施方式

[0072] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0073] 参照图1,本发明一实施例中提供了一种显示器的身份校验方法,包括以下步骤:

[0074] 步骤S1,获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;

[0075] 步骤S2,获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;

[0076] 步骤S3,基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;

[0077] 步骤S4,将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;

[0078] 步骤S5,对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库

中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;

[0079] 步骤S6,若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。

[0080] 在本实施例中,上述方案应用于显示器上对用户的使用权限进行校验,校验过程中,结合了加密和哈希算法,有效地保护用户的隐私和安全,同时快速、准确地处理用户提交的身份验证信息,提高身份验证的效率和准确性。

[0081] 具体地,如上述步骤S1所述的,可以使用一个表单或者界面来获取用户的身份验证信息,比如用户名、密码、指纹等。获取到用户的身份验证信息后,需要对其进行分割,将其分成第一身份信息和第二身份信息。这个分割规则可以根据具体的业务需求来制定,比如可以按照字符数、空格、特殊符号等进行分割。

[0082] 如上述步骤S2所述的,在获取设备类型时,可以通过调用API或者系统函数来获取设备类型。获取到设备类型后,需要在数据库中查找与之对应的加密密钥。在数据库中存储了设备类型与第一加密密钥、第二加密密钥的映射关系,因此只需要根据设备类型来查询相应的加密密钥即可。

[0083] 如上述步骤S3所述的,在获取到加密密钥后,需要对第一身份信息和第二身份信息进行加密。这里可以使用对称加密算法,比如AES算法。根据所述第一加密密钥和第二加密密钥,分别对第一身份信息和第二身份信息进行加密,得到第一加密数据和第二加密数据。本实施例中,针对不同的身份信息,采用不同的加密密钥,提升了身份信息的安全性、私密性。

[0084] 如上述步骤S4所述的,将第一加密数据和第二加密数据进行拼接,得到拼接加密数据。这个过程可以使用字符串拼接函数来实现。

[0085] 如上述步骤S5所述的,对拼接加密数据进行哈希计算,得到对应的拼接哈希值;这里可以使用SHA-256等哈希算法。然后,在数据库中遍历哈希值列表,查询是否存在与拼接哈希值相同的哈希值。

[0086] 如上述步骤S6所述的,如果在哈希值列表中找到了与拼接哈希值相同的哈希值,说明用户具有使用该显示器的使用权限。否则,用户不具有使用该显示器的使用权限。进一步地,根据判断结果,可以向用户展示相应的提示信息。在本实施例中,基于结合了加密和哈希算法,有效地保护用户的隐私和安全,同时采用哈希值的匹配对比方式,快速、准确地处理用户提交的身份验证信息,提高身份验证的效率和准确性。

[0087] 在一实施例中,所述判定所述用户具有使用所述显示器的使用权限的步骤S6之后,包括:

[0088] 步骤S7,生成一个二维码,并将所述第一身份信息以及第二身份信息添加在所述二维码中;

[0089] 步骤S8,将所述二维码发送至所述用户所持的智能终端上;其中,所述用户在下一次使用所述显示器时,只需要出示所述二维码,无需再次输入身份验证信息。

[0090] 在本实施例中,为了方便具有显示器控制权限的用户后续快速访问显示器,可以生成一个具备控制权限的二维码,将所述第一身份信息以及第二身份信息添加在所述二维码中,再将二维码发送至用户所持的智能终端上;其中,所述用户在下一次使用所述显示器时,只需要出示所述二维码至显示器前即可,显示器通过扫描上述二维码,便可以验证对应

的权限。

[0091] 在一实施例中,所述生成一个二维码,并将所述第一身份信息以及第二身份信息添加在所述二维码中的步骤,包括:

[0092] 导入QR Code生成库;

[0093] 获取所述第一身份信息以及第二身份信息的数据类型,并根据所述数据类型,选择对应的纠错级别;其中,数据库存储有数据类型与纠错级别的映射关系;其中,数据类型和纠错级别的选择是保证二维码可靠性和识别速度的重要因素。

[0094] 获取所述第一身份信息以及第二身份信息的总数据量,获取所述显示器前方的空间距离;根据所述总数据量以及所述空间距离,确定二维码的尺寸和版本;上述二维码的尺寸和版本主要由总数据量以及所述空间距离所确定。

[0095] 基于QR Code生成库以及所述纠错级别,将所述第一身份信息以及第二身份信息编码成对应尺寸以及版本的二维码矩阵;在本实施例中,上述QR Code生成库(一种生成和解析二维码的js库)可以自动化地将第一身份信息和第二身份信息编码成对应尺寸和版本的二维码矩阵。

[0096] 对所述二维码矩阵进行错误校验并生成最终的二维码,将生成的二维码保存为图像文件。

[0097] 在本实施例中,采用了先进的QR Code生成库和自动计算二维码尺寸和版本的方法,能够快速、准确地生成高质量的二维码。同时,该方案还考虑了不同数据类型和空间距离对二维码识别的影响,选择合适的纠错级别和尺寸版本,从而提高了二维码的可靠性和识别速度。

[0098] 在一实施例中,所述获取用户输入的身份验证信息的步骤S1,包括:

[0099] 接收用户所持终端依序发送的多个数据包,多个数据包按照发送顺序组成数据包序列;在本实施例中,需要先接收用户所持终端依序发送的多个数据包,并按照发送顺序组成数据包序列。

[0100] 对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括空白数据包;

[0101] 若包括空白数据包,则检测出包括空白数据包的数据包数量为x,作为第一数量;对于数据包序列中的每个数据包,需要进行检测,判断其是否为空白数据包。如果检测到数据包中包含空白数据包,则记录下该数据包的数量x,并作为第一数量。

[0102] 从所述数据包序列中,检测出排列在第x位上的目标数据包;

[0103] 对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息。从数据包序列中找出排列在第x位上的目标数据包,并进行解析,以获取其中携带的身份验证信息。解析过程中需要注意保证数据的完整性和正确性,避免因数据传输错误或恶意篡改导致身份验证失败。

[0104] 在本实施例中,采用了逐个检测数据包的方式,可以有效避免因丢失或重复接收数据包而导致身份验证失败的问题。同时,通过检测空白数据包的数量,可以快速定位到目标数据包,提高了身份验证的效率和准确性。

[0105] 在一实施例中,所述对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息的步骤,包括:

[0106] 对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括指定的干扰数据包;其中,所述干扰数据包是各个数据包中未加密且携带有数据的数据包;在本实施例中,需要逐个检测各个数据包中是否包括指定的干扰数据包。

[0107] 若包括干扰数据包,则检测出干扰数据包的数据包数量,作为第二数量;对于每个包含干扰数据包的数据包,记录其所在位置,以及包含的干扰数据包的第二数量。该第二数量用于结合第一数量进行目标数据包的解析过程。

[0108] 基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;编码表可以采用任何公开的或自定义的编码方式,例如ASCII码、二进制编码等。

[0109] 将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为解密密码对所述目标数据包进行解密,得到所述目标数据包中携带的身份验证信息;其中,所述数据包序列中只有所述目标数据包为加密数据。组合方式可以采用任何公开的或自定义的组合方式,例如按位异或、拼接等。

[0110] 在本实施例中,基于上述数据包序列中空白数据包的第一数量以及干扰数据包的第二数量,进行编码、组合得到对应的解密密码,使得无需存储解密密码,只需要通过上述数据包序列便可以得到,提升了密码安全性。

[0111] 在本实施例中,所述用户所持终端依序发送的多个数据包,包括:

[0112] 所述用户所持终端接收用户输入的所述身份验证信息;

[0113] 将所述身份验证信息添加至一个数据包中,得到身份数据包;

[0114] 随机生成第二数量的干扰身份信息,并将所述干扰身份信息添加在数据包中,得到第二数量的干扰数据包;上述干扰身份信息用于产生干扰,增加破解难度,提高安全性。

[0115] 生成第一数量的空白数据包;

[0116] 将所有所述干扰数据包与所述空白数据包随机进行排序,得到第一数据包序列;这样可以增加数据的随机性和安全性,使攻击者不能轻易地猜测数据包的位置和内容。

[0117] 基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

[0118] 将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为加密密码对所述身份数据包进行加密,得到目标数据包;数据包经过加密和随机排序等,以提高身份验证的安全性和可靠性。

[0119] 将所述目标数据包插入至所述第一数据包序列中,并使得所述目标数据包位于第x位上,得到第二数据包序列;

[0120] 基于所述第二数据包序列,依次发送各个数据包至显示器。基于上述方式,实现安全的身份验证和数据保护。

[0121] 参照图2,本发明一实施例中还提供了一种显示器的身份校验装置,包括:

[0122] 第一获取单元,用于获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;

[0123] 第二获取单元,用于获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;

[0124] 加密单元,用于基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;

[0125] 拼接单元,用于将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;

[0126] 计算单元,用于对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;

[0127] 判定单元,用于若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。

[0128] 在一实施例中,所述第一获取单元,包括:

[0129] 接收子单元,用于接收用户所持终端依序发送的多个数据包,多个数据包按照发送顺序组成数据包序列;

[0130] 第一检测子单元,用于对所述数据包序列中的数据包分别进行检测,检测各个数据包中是否包括空白数据包;

[0131] 第二检测子单元,用于若包括空白数据包,则检测出包括空白数据包的数据包数量为x,作为第一数量;

[0132] 第三检测子单元,用于从所述数据包序列中,检测出排列在第x位上的目标数据包;

[0133] 解析子单元,用于对所述目标数据包进行解析,获取所述目标数据包中携带的身份验证信息。

[0134] 在一实施例中,所述用户所持终端依序发送的多个数据包,包括:

[0135] 所述用户所持终端接收用户输入的所述身份验证信息;

[0136] 将所述身份验证信息添加至一个数据包中,得到身份数据包;

[0137] 随机生成第二数量的干扰身份信息,并将所述干扰身份信息添加在数据包中,得到第二数量的干扰数据包;

[0138] 生成第一数量的空白数据包;

[0139] 将所有所述干扰数据包与所述空白数据包随机进行排序,得到第一数据包序列;

[0140] 基于预设的编码表,对所述第一数量以及第二数量分别进行编码,得到对应的第一编码以及第二编码;

[0141] 将所述第一编码以及第二编码进行组合,得到组合编码,将所述组合编码作为加密密码对所述身份数据包进行加密,得到目标数据包;

[0142] 将所述目标数据包插入至所述第一数据包序列中,并使得所述目标数据包位于第x位上,得到第二数据包序列;

[0143] 基于所述第二数据包序列,依次发送各个数据包至显示器。

[0144] 在本实施例中,上述装置实施例中的各个单元的具体实现,请参照上述方法实施例中所述,在此不再进行赘述。

[0145] 参照图3,本发明实施例中还提供一种计算机设备,该计算机设备可以是服务器,其内部结构可以如图3所示。该计算机设备包括通过系统总线连接的处理器、存储器、显示屏、输入装置、网络接口和数据库。其中,该计算机设计的处理器用于提供计算和控制能力。

该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储本实施例中对应的数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种显示器的身份校验方法。

[0146] 本领域技术人员可以理解,图3中示出的结构,仅仅是与本发明方案相关的部分结构的框图,并不构成对本发明方案所应用于其上的计算机设备的限定。

[0147] 本发明一实施例还提供一种计算机可读存储介质,其上存储有计算机程序,计算机程序被处理器执行时实现一种显示器的身份校验方法。可以理解的是,本实施例中的计算机可读存储介质可以是易失性可读存储介质,也可以为非易失性可读存储介质。

[0148] 综上所述,为本发明实施例中提供的显示器的身份校验方法、装置、计算机设备和存储介质,包括:获取用户输入的身份验证信息,并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息;获取显示器的设备类型,基于所述设备类型从数据库中获取两个预设的加密密钥,分别为第一加密密钥以及第二加密密钥;其中,数据库中存储有设备类型与第一加密密钥、第二加密密钥的映射关系;基于所述第一加密密钥对所述第一身份信息进行加密,得到第一加密数据;基于第二加密密钥对所述第二身份信息进行加密,得到第二加密数据;将所述第一加密数据与第二加密数据进行拼接,得到拼接加密数据;对所述拼接加密数据进行哈希计算,得到对应的拼接哈希值;遍历数据库中的哈希值列表,查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值;若包括,则判定所述用户具有使用所述显示器的使用权限;若不包括,则判定所述用户不具有使用所述显示器的使用权限。本发明中,结合了加密和哈希算法,有效地保护用户的隐私和安全,同时快速、准确地处理用户提交的身份验证信息,提高身份验证的效率和准确性。

[0149] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的计算机程序可存储于一非易失性计算机可读取存储介质中,该计算机程序在执行时,可包括如上述各方法的实施例的流程。其中,本发明所提供的和实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可以包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM通过多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双速据率SDRAM(SSRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM等。

[0150] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其它变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、装置、物品或者方法不仅包括那些要素,而且还包括没有明确列出的其它要素,或者是还包括为这种过程、装置、物品或者方法所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、装置、物品或者方法中还存在另外的相同要素。

[0151] 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它相关

的技术领域,均同理包括在本发明的专利保护范围内。

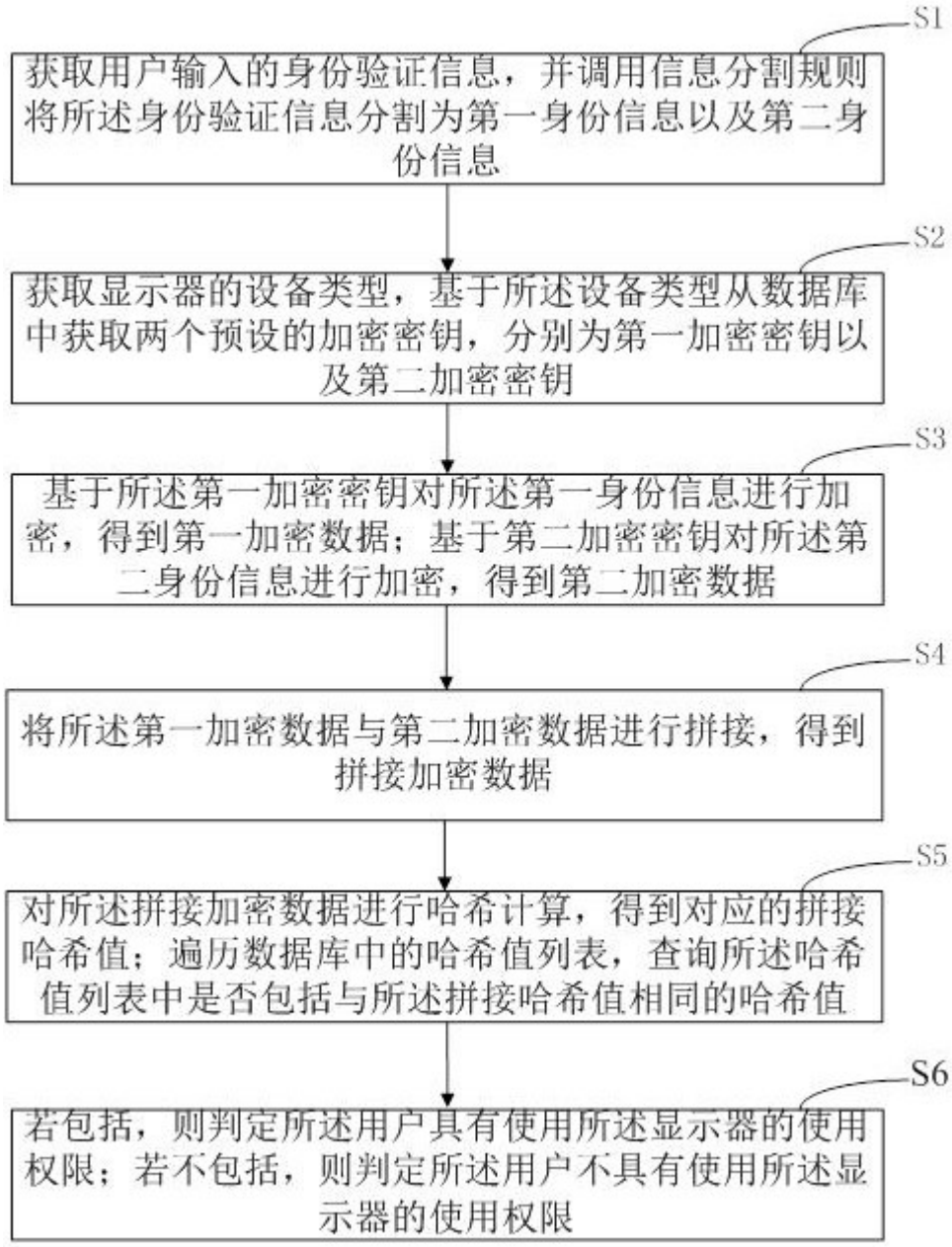

S1
获取用户输入的身份验证信息，并调用信息分割规则将所述身份验证信息分割为第一身份信息以及第二身份信息
S2
获取显示器的设备类型，基于所述设备类型从数据库中获取两个预设的加密密钥，分别为第一加密密钥以及第二加密密钥
S3
基于所述第一加密密钥对所述第一身份信息进行加密，得到第一加密数据；基于第二加密密钥对所述第二身份信息进行加密，得到第二加密数据
S4
将所述第一加密数据与第二加密数据进行拼接，得到拼接加密数据
S5
对所述拼接加密数据进行哈希计算，得到对应的拼接哈希值；遍历数据库中的哈希值列表，查询所述哈希值列表中是否包括与所述拼接哈希值相同的哈希值
S6
若包括，则判定所述用户具有使用所述显示器的使用权限；若不包括，则判定所述用户不具有使用所述显示器的使用权限

图1

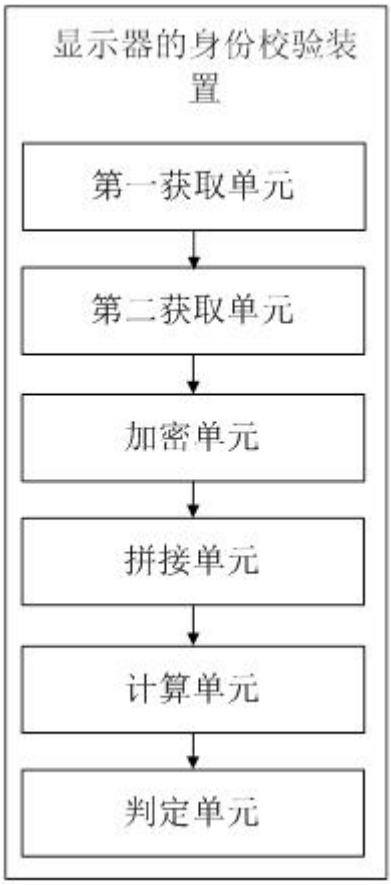


图2

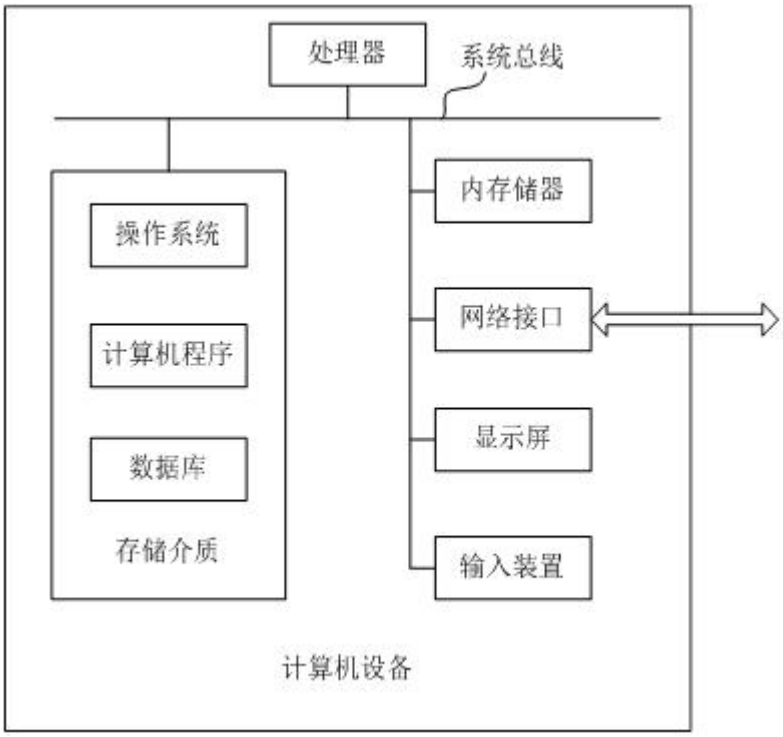


图3