



(12) 发明专利申请

(10) 申请公布号 CN 105069365 A

(43) 申请公布日 2015. 11. 18

(21) 申请号 201510386842. X

(22) 申请日 2015. 06. 30

(71) 申请人 广东欧珀移动通信有限公司

地址 523860 广东省东莞市长安镇乌沙海滨路 18 号

(72) 发明人 张海平

(74) 专利代理机构 广州三环专利代理有限公司

44202

代理人 郝传鑫 熊永强

(51) Int. Cl.

G06F 21/62(2013. 01)

G06F 21/78(2013. 01)

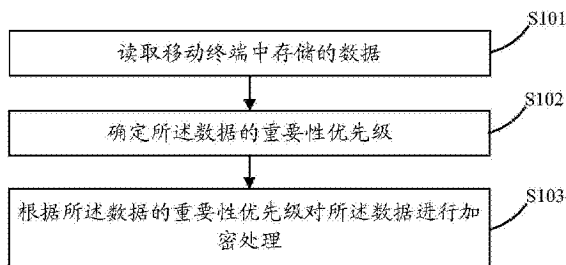
权利要求书2页 说明书9页 附图3页

(54) 发明名称

一种数据处理的方法及移动终端

(57) 摘要

本发明实施例公开了一种数据加密的方法,包括:读取移动终端中存储的数据;确定所述数据的重要性优先级;根据所述数据的重要性优先级对所述数据进行加密处理。本发明实施例还公开了一种移动终端。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。



1. 一种数据处理的方法,其特征在于,包括:

读取移动终端中存储的数据;

确定所述数据的重要性优先级;

根据所述数据的重要性优先级对所述数据进行加密处理。

2. 如权利要求 1 所述的方法,所述确定所述数据的重要性优先级,包括:

获取所述数据关联的标记信息;

将所述标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。

3. 如权利要求 1 所述的方法,其特征在于,所述重要性优先级至少包括第一优先级和第二优先级,其中,所述第一优先级高于所述第二优先级,所述根据所述数据的重要性优先级对所述数据进行加密处理,包括:

在所述数据的重要性优先级为所述第一优先级的情况下,根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据;

或者,

在所述数据的重要性优先级为所述第二优先级的情况下,根据第二加密算法和预设第二密钥对所述数据进行第二加密处理以得到第二加密数据。

4. 如权利要求 3 所述的方法,其特征在于,所述预设第一密钥为以下至少一种:指纹信息、虹膜信息、人脸信息和指纹信息、虹膜信息、人脸信息及字符密码中的至少两者组合作为密钥;

所述预设第二密钥为用户针对所述数据设置的字符密码或者移动终端的标识信息。

5. 如权利要求 3 所述的方法,其特征在于,所述第一加密算法包括如下加密算法中的至少一种:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 和高级加密标准 AES;

所述第二加密算法包括如下加密算法中的至少一种:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 和高级加密标准 AES。

6. 一种移动终端,其特征在于,包括:

读取单元,用于读取移动终端中存储的数据;

确定单元,用于确定所述读取单元读取的数据的重要性优先级;

加密单元,用于根据所述确定单元确定的数据的重要性优先级对所述数据进行加密处理。

7. 如权利要求 6 所述的方法,所述确定单元包括:

获取单元,用于获取所述读取单元读取的数据关联的标记信息;

对比单元,用于将所述获取单元获取到的标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。

8. 如权利要求 6 所述的方法,其特征在于,所述重要性优先级至少包括第一优先级和第二优先级,其中,所述第一优先级高于所述第二优先级,所述加密单元具体用于:

在所述数据的重要性优先级为所述第一优先级的情况下,根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据;

或者,

在所述数据的重要性优先级为所述第二优先级的情况下,根据第二加密算法和预设第二密钥对所述数据进行第二加密处理以得到第二加密数据。

9. 如权利要求 8 所述的移动终端,其特征在于,所述预设第一密钥为以下至少一种:指纹信息、虹膜信息、人脸信息和指纹信息、虹膜信息、人脸信息及字符密码中的至少两者组合作为密钥;

所述预设第二密钥为用户针对所述数据设置的字符密码或者移动终端的标识信息。

10. 如权利要求 8 所述的移动终端,其特征在于,所述第一加密算法包括如下加密算法中的至少一种:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 和高级加密标准 AES;

所述第二加密算法包括如下加密算法中的至少一种:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 和高级加密标准 AES。

一种数据处理的方法及移动终端

技术领域

[0001] 本发明实施例涉及电子设备技术领域,尤其涉及到一种数据处理的方法及移动终端。

背景技术

[0002] 随着科技的发展,移动终端(如手机、平板电脑、智能穿戴设备等等)越来越普及,同时,功能也越来越强大,已从一种单纯的通信工具演变成为一种集成多功能的电子便携设备。

[0003] 生活中,在对移动终端中的不同数据进行不同的加密的过程中,不同的数据可能采用不同的加密方式,从而,会出现下述情况,有的数据可能采用数字加密,有的数据可能采用指纹加密,有的数据可能采用语音加密,因而,数据采用多种不同方式进行加密较为繁琐,且容易忘记密码。

发明内容

[0004] 本发明实施例提供了一种数据处理的方法及移动终端,以期在对数量较多的数据都进行加密的过程中,简化加密过程,同时,使得加密中使用的密码较容易记住。

[0005] 本发明实施例第一方面公开了一种数据处理的方法,包括:

[0006] 读取移动终端中存储的数据;

[0007] 确定所述数据的重要性优先级;

[0008] 根据所述数据的重要性优先级对所述数据进行加密处理。

[0009] 相应地,本发明实施例第二方面公开了一种移动终端,包括:

[0010] 读取单元,用于读取移动终端中存储的数据;

[0011] 确定单元,用于确定所述读取单元读取的数据的重要性优先级;

[0012] 加密单元,用于根据所述确定单元确定的数据的重要性优先级对所述数据进行加密处理。

[0013] 本发明实施例读取移动终端中存储的数据;确定所述数据的重要性优先级;根据所述数据的重要性优先级对所述数据进行加密处理。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。

附图说明

[0014] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例、描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明实施例的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

- [0015] 图 1 为本发明实施例提供的一种数据处理的方法的第一实施例的流程示意图；
- [0016] 图 2 为本发明实施例提供的一种数据处理的方法的第二实施例的流程示意图；
- [0017] 图 3 为本发明实施例提供的一种数据处理的方法的第三实施例的流程示意图；
- [0018] 图 4a 为本发明实施例提供的一种移动终端的第一实施例的结构示意图；
- [0019] 图 4b 为本发明实施例提供的一种移动终端的第一实施例的又一结构示意图；
- [0020] 图 5 为本发明实施例提供的一种移动终端的第二实施例的结构示意图。

具体实施方式

[0021] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明实施例一部分实施例,而不是全部的实施例。基于本发明实施例中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明实施例保护的范畴。

[0022] 实现中,本发明实施例中,移动终端可以包括但不限于:笔记本电脑、手机、平板电脑、智能可穿戴设备等等。移动终端的系统指设备的操作系统,可以包括但不限于:Android 系统、塞班系统、Windows 系统、IOS(苹果公司开发的移动操作系统)、XP 系统、windows 8 系统等等。需要说明的是,Android 移动终端指 Android 系统的移动终端,塞班移动终端指塞班系统的移动终端,等等。上述移动终端仅是举例,而非穷举,包含但不限于上述移动终端。

[0023] 本发明实施例结合图 1 至图 5 对本发明实施例提供的一种数据处理的方法及移动终端进行描述。

[0024] 请参阅图 1,图 1 是本发明实施例提供的一种数据处理的方法的第一实施例流程示意图。本实施例中所描述的数据处理的方法,包括以下步骤:

[0025] S101、读取移动终端中存储的数据。

[0026] 具体实现中,移动终端可读取该移动终端中存储的数据。实际应用中,并不是所有的数据都需要加密,一般情况下,需加密的数据都是重要数据或者出于私隐目的不便于外人查阅的数据。可选地,数据的类型可包括但不限于:word 数据、excel 数据、图片数据、视频数据、音频数据、文件夹、应用程序、桌面快捷方式等。

[0027] S102、确定所述数据的重要性优先级。

[0028] 具体实现中,移动终端可确定数据的重要性优先级,进一步地,重要性优先级可分为第一优先级、第二优先级、第三优先级。其中,第一优先级高于第二优先级,第二优先级高于第三优先级。通常情况下,可认为第一优先级数据相当于移动终端中重要性最高的数据,该数据解密难度最大,可认为该部分数据不希望别人轻易看到;第二优先级数据相当于移动终端中一般的重要数据,但是该部分数据可以让好朋友看到,该部分数据解密难度相对第一优先级较小;而第三优先级可理解为普通数据,该部分数据可以公开。

[0029] 可选地,移动终端可通过用户对数据进行标记方式的确定该数据的重要性优先级,例如,用户将移动终端读取的数据标记为第一优先级。进一步可选地,倘若不重要的数据,用户可对该数据不进行标记。

[0030] 可选地,移动终端可通过根据数据的类型确定数据的重要性优先级,例如,可将图片数据为第一优先级,或者,可将视频数据确定为第二优先级。进一步可选地,倘若不重要

的数据,则可不比确定该数据的优先级。

[0031] S103、根据所述数据的重要性优先级对所述数据进行加密处理。

[0032] 具体实现中,移动终端可根据确定的数据的重要性优先级对该数据进行加密处理,如该数据为第一优先级,可采用第一优先级的加密方式对该数据进行第一加密处理。

[0033] 例如,移动终端对数据进行加密的时候,移动终端可先读取移动终端中存储的数据,再确定该数据的重要性优先级;根据该数据的重要性优先级对该数据进行加密处理。即,假设移动终端读取了M个数据,其中,N个数据为第一优先级的数据,M大于N,且N大于1,M与N均为整数,则移动终端可采用第一优先级对应的第一加密算法和第一密钥对该N个数据进行加密,其中,N个密钥可由系统预先设置,因而,不必在每次确定了数据的重要性优先级都得获取密钥,从而,N个数据可采用同一密钥进行加密,这在解密过程中,用户不需要记住太多的密码。即移动终端只要确定了其读取的数据的重要性优先级,便可以根据该数据的重要性优先级对该数据进行加密。

[0034] 本发明实施例读取移动终端中存储的数据;确定所述数据的重要性优先级;根据所述数据的重要性优先级对所述数据进行加密处理。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。

[0035] 请参阅图2,图2是本发明实施例提供的一种数据处理的方法的第二实施例流程示意图。本实施例中所描述的数据处理的方法,包括以下步骤:

[0036] S201、读取移动终端中存储的数据。

[0037] 具体实现中,移动终端可读取该移动终端中存储的数据。实际应用中,并不是所有的数据都需要加密,一般情况下,需加密的数据都是重要数据或者出于私隐目的不便于外人查阅的数据。可选地,数据的类型可包括但不限于:word数据、excel数据、图片数据、视频数据、音频数据、文件夹、应用程序、桌面快捷方式等。

[0038] S202、获取所述数据关联的标记信息。

[0039] 具体实现中,移动终端可获取数据关联的标记信息,数据关联的标记信息可为:数据类型(即图片、视频、网页等等)、数据日期、数据大小、数据来源、数据版本等等。

[0040] S203、将所述标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。

[0041] 具体实现中,移动终端可将标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。例如,预置的重要性优先级列表可形如:图片第一优先级、视频第二优先级。紧接着,假设,移动终端读取的数据关联的标记信息为图片,移动终端可将该标识信息与预置的重要性优先级列表进行比对,从而,可确定该数据的重要性优先级为第一优先级。

[0042] S204、根据所述数据的重要性优先级对所述数据进行加密处理。

[0043] 具体实现中,移动终端可根据确定的数据的重要性优先级对该数据进行加密处理,如该数据为第一优先级,可采用第一优先级的加密方式对该数据进行第一加密处理。

[0044] 本发明实施例读取移动终端中存储的数据;获取所述数据关联的标记信息;将所述标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级;根据所

述数据的重要性优先级对所述数据进行加密处理。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。

[0045] 请参阅图 3,图 3 是本发明实施例提供的一种数据处理的方法的第三实施例流程示意图。本实施例中所述的数据处理的方法,包括以下步骤:

[0046] S301、读取移动终端中存储的数据。

[0047] 具体实现中,移动终端可读取该移动终端中存储的数据。实际应用中,并不是所有的数据都需要加密,一般情况下,需加密的数据都是重要数据或者出于私隐目的不便于外人查阅的数据。可选地,数据的类型可包括但不限于:word 数据、excel 数据、图片数据、视频数据、音频数据、文件夹、应用程序、桌面快捷方式等。

[0048] S302、确定所述数据的重要性优先级。

[0049] 具体实现中,移动终端可确定数据的重要性优先级,进一步地,重要性优先级可分为第一优先级、第二优先级、第三优先级。其中,第一优先级高于第二优先级,第二优先级高于第三优先级。通常情况下,可认为第一优先级数据相当于移动终端中重要性最高的数据,该数据解密难度最大,可认为该部分数据不希望别人轻易看到;第二优先级数据相当于移动终端中一般的重要数据,但是该部分数据可以让好朋友看到,该部分数据解密难度相对第一优先级较小;而第三优先级可理解为普通数据,该部分数据可以公开。

[0050] 可选地,移动终端可通过用户对数据进行标记方式的确定该数据的重要性优先级,例如,用户将移动终端读取的数据标记为第一优先级。进一步可选地,倘若不重要的数据,用户可对该数据不进行标记。

[0051] 可选地,移动终端可通过根据数据的类型确定数据的重要性优先级,例如,可将自图片数据为第一优先级,或者,可将视频数据确定为第二优先级。进一步可选地,倘若不重要的数据,则可不比确定该数据的优先级。

[0052] S303、在所述数据的重要性优先级为所述第一优先级的情况下,根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据。

[0053] 具体实现中,移动终端可根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据。可选地,第一加密算法可包括但不限于:数据加密算法(英文:Data Encryption Standard,缩写:DES)、国际数据加密算法(英文:International Data Encryption Algorithm,缩写:IDEA)、RSA、单向散列算法(英文:Message-Digest Algorithm 5,缩写:MD5)、数字签名算法(英文:Digital Signature Algorithm,缩写:DSA)或高级加密标准(英文:Advanced Encryption Standard,缩写:AES)等。

[0054] 进一步地,在数据的重要性优先级为第二优先级的情况下,移动终端可根据第二加密算法和预设第二密钥对数据进行第二加密处理以得到第二加密数据。可选地,第二加密算法可包括但不限于:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 或高级加密标准 AES。可选地,预设第二密钥为用户针对数据设置的字符密码或者移动终端的标识信息。其中,移动终端的标识信息可包括但不限于:国际移动设备身份码(International Mobile Equipment Identity,IMEI)、移动终端识别的电话号码、集成电路卡识别码(Integrate Circuit Card Identity, ICCID)和移动终端入网许

可号。可选地,移动终端识别的电话号码可以是多个,例如,双卡双待的手机可以插入两张卡。可选地,移动终端的标识信息可以是国际移动设备身份码 IMEI、移动终端识别的电话号码、集成电路卡识别码 ICCID 和移动终端入网许可号中的两两组合或者其他任意组合。可选地,用户针对数据设置的字符密码可包括但不限于:数字、字母或符号。可选地,用户对文件设置的字符密码长度可包括但不限于:1位,2位,3位-8位,6位-8位,不小于3位等。

[0055] 例如,移动终端确定了读取的数据的重要性优先级为第一优先级,第一密钥为用户输入的指纹信息。如移动终端对一张图片进行加密,第一密钥选择用户输入的左手中指的指纹信息,第一加密算法选择 RSA,则移动终端可根据第一加密算法 RSA 和用户输入的左手中指的指纹信息对图片进行加密。

[0056] 本发明实施例读取移动终端中存储的数据;确定所述数据的重要性优先级;在所述数据的重要性优先级为所述第一优先级的情况下,根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。

[0057] 请参见图 4a,图 4a 为本发明实施例提供的一种移动终端的第一实施例的结构示意图,图 4a 所描述的移动终端可包括:读取单元 401、确定单元 402 和加密单元 403,具体如下:

[0058] 读取单元 401,用于读取移动终端中存储的数据。

[0059] 具体实现中,读取单元 401 可读取该移动终端中存储的数据。实际应用中,并不是所有的数据都需要加密,一般情况下,需加密的数据都是重要数据或者出于私隐目的不便于外人查阅的数据。可选地,数据的类型可包括但不限于:word 数据、excel 数据、图片数据、视频数据、音频数据、文件夹、应用程序、桌面快捷方式等。

[0060] 确定单元 402,用于确定所述读取单元 401 读取的数据的重要性优先级。

[0061] 具体实现中,确定单元 402 可确定数据的重要性优先级,进一步地,重要性优先级可分为第一优先级、第二优先级、第三优先级。其中,第一优先级高于第二优先级,第二优先级高于第三优先级。通常情况下,可认为第一优先级数据相当于移动终端中重要性最高的数据,该数据解密难度最大,可认为该部分数据不希望别人轻易看到;第二优先级数据相当于移动终端中一般的重要数据,但是该部分数据可以让好朋友看到,该部分数据解密难度相对第一优先级较小;而第三优先级可理解为普通数据,该部分数据可以公开。

[0062] 可选地,确定单元 402 可通过用户对数据进行标记方式的确定该数据的重要性优先级,例如,用户将移动终端读取的数据标记为第一优先级。进一步可选地,倘若不重要的数据,用户可对该数据不进行标记。

[0063] 可选地,确定单元 402 可通过根据数据的类型确定数据的重要性优先级,例如,可将自图片数据为第一优先级,或者,可将视频数据确定为第二优先级。进一步可选地,倘若不重要的数据,则可不比确定该数据的优先级。

[0064] 加密单元 403,用于根据所述确定单元 402 确定的数据的重要性优先级对所述数据进行加密处理。

[0065] 具体实现中,加密单元 403 可根据确定的数据的重要性优先级对该数据进行加密处理,如该数据为第一优先级,可采用第一优先级的加密方式对该数据进行第一加密处理。

[0066] 例如,加密单元 403 对数据进行加密的过程中,读取单元 401 可先读取移动终端中存储的数据,确定单元 402 再确定该数据的重要性优先级;加密单元 403 根据该数据的重要性优先级对该数据进行加密处理。即,假设读取单元 401 读取了 M 个数据,其中, N 个数据为第一优先级的数据, M 大于 N,且 N 大于 1, M 与 N 均为整数,则移动终端可采用第一优先级对应的第一加密算法和第一密钥对该 N 个数据进行加密,其中, N 个密钥系统可预先设置,因而,不必在每次确定了数据的重要性优先级都得获取密钥,从而, N 个数据可采用同一密钥进行加密,这在解密过程中,用户不需要记住太多的密码。即确定单元 402 只要确定了其读取的数据的重要性优先级,便可以根据该数据的重要性优先级对该数据进行加密。

[0067] 作为一种可能的实施方式,如图 4b 所示,图 4a 中所描述的移动终端的确定单元 402 可包括:获取单元 4021 和对比单元 4022,具体如下:

[0068] 获取单元 4021,用于获取所述读取单元 401 读取的数据关联的标记信息。

[0069] 具体实现中,获取单元 4021 可获取数据关联的标记信息,数据关联的标记信息可为:数据类型(即图片、视频、网页等等)、数据日期、数据大小、数据来源、数据版本等等。

[0070] 对比单元 4022,用于将所述获取单元 4021 获取到的标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。

[0071] 具体实现中,对比单元 4022 可将标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。例如:预置的重要性优先级列表可形如:图片第一优先级、视频第二优先级。紧接着,假设,获取单元 4021 获取到了读取单元 401 读取的数据关联的标记信息为图片,则对比单元 4022 可将该标记信息和预置的重要性优先级列表进行比对可确定该数据的重要性优先级为第一优先级。

[0072] 作为一种可能的实施方式,在数据的重要性优先级为第一优先级的情况下,加密单元 403 可根据第一加密算法和预设第一密钥对数据进行第一加密处理以得到第一加密数据。

[0073] 具体实现中,移动终端可根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据。可选地,第一加密算法可包括但不限于:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 或高级加密标准 AES。

[0074] 例如,确定单元 402 确定了读取的数据的重要性优先级为第一优先级,第一密钥为用户输入的指纹信息。如移动终端对一张图片进行加密,第一密钥选择用户输入的左手中指的指纹信息,第一加密算法选择 RSA,则加密单元 403 可根据第一加密算法 RSA 和用户输入的左手中指的指纹信息对图片进行加密。

[0075] 作为一种可能的实施方式,在数据的重要性优先级为第二优先级的情况下,加密单元 403 可根据第二加密算法和预设第二密钥对数据进行第二加密处理以得到第二加密数据。

[0076] 具体实现中,在数据的重要性优先级为第二优先级的情况下,移动终端可根据第二加密算法和预设第二密钥对数据进行第二加密处理以得到第二加密数据。可选地,第二加密算法可包括但不限于:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算

法 MD5、数字签名算法 DSA 或高级加密标准 AES。可选地,预设第二密钥为用户针对数据设置的字符密码或者移动终端的标识信息。其中,移动终端的标识信息可包括但不限于:国际移动设备身份码 IMEI、移动终端识别的电话号码、集成电路卡识别码 ICCID 和移动终端入网许可号。可选地,移动终端识别的电话号码可以是多个,例如,双卡双待的手机可以插入两张卡。可选地,移动终端的标识信息可以是国际移动设备身份码 IMEI、移动终端识别的电话号码、集成电路卡识别码 ICCID 和移动终端入网许可号中的两两组合或者其他任意组合。可选地,用户针对数据设置的密码可包括但不限于:数字、字母或符号。可选地,用户对文件设置的密码长度可包括但不限于:1 位,2 位,3 位-8 位,6 位-8 位,不小于 3 位等。

[0077] 本发明实施例所描述的终端通过读取移动终端中存储的数据;确定所述数据的重要性优先级;根据所述数据的重要性优先级对所述数据进行加密处理。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。

[0078] 请参阅图 5,图 5 为本发明实施例提供的一种移动终端的第二实施例的结构示意图。本实施例中所描述的移动终端包括:至少一个输入设备 1000;至少一个输出设备 2000;至少一个处理器 3000,例如 CPU;和存储器 4000,上述输入设备 1000、输出设备 2000、处理器 3000 和存储器 4000 通过总线 5000 连接。

[0079] 其中,上述输入设备 1000 可为触控面板、普通 PC、液晶屏、触控屏、触控按钮等。

[0080] 上述存储器 4000 可以是高速 RAM 存储器,也可为非不稳定的存储器(non-volatile memory),例如磁盘存储器。上述存储器 4000 用于存储一组程序代码,上述输入设备 1000、输出设备 2000 和处理器 3000 用于调用存储器 4000 中存储的程序代码,执行如下操作:

[0081] 上述处理器 3000,用于:

[0082] 读取移动终端中存储的数据;

[0083] 确定所述数据的重要性优先级;

[0084] 根据所述数据的重要性优先级对所述数据进行加密处理。

[0085] 在一些可行的实施方式中,上述处理器 3000 确定所述数据的重要性优先级,具体为:

[0086] 获取所述数据关联的标记信息;

[0087] 将所述标记信息与预置的重要性优先级列表进行比对以得到所述数据的重要性优先级。

[0088] 在一些可行的实施方式中,若重要性优先级至少包括第一优先级和第二优先级,且第一优先级高于所述第二优先级,上述处理器 3000 根据所述数据的重要性优先级对所述数据进行加密处理,具体为:

[0089] 在所述数据的重要性优先级为所述第一优先级的情况下,根据第一加密算法和预设第一密钥对所述数据进行第一加密处理以得到第一加密数据;

[0090] 或者,

[0091] 在所述数据的重要性优先级为所述第二优先级的情况下,根据第二加密算法和预设第二密钥对所述数据进行第二加密处理以得到第二加密数据。

[0092] 作为一种可能的实施方式,预设第一密钥为以下至少一种:指纹信息、虹膜信息、人脸信息和指纹信息、虹膜信息、人脸信息及字符密码中的至少两者组合作为密钥;

[0093] 作为一种可能的实施方式,预设第二密钥为用户针对数据设置的字符密码或者移动终端的标识信息。

[0094] 作为一种可能的实施方式,第一加密算法可包括但不限于:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 和高级加密标准 AES;

[0095] 作为一种可能的实施方式,第二加密算法可包括但不限于:数据加密算法 DES、国际数据加密算法 IDEA、RSA、单向散列算法 MD5、数字签名算法 DSA 和高级加密标准 AES。

[0096] 本发明实施例所描述的移动终端通过读取移动终端中存储的数据;确定所述数据的重要性优先级;根据所述数据的重要性优先级对所述数据进行加密处理。如此,可根据确定的数据的重要性优先级对数据进行加密,从而,在对数量较多的数据进行加密的过程中,使用数据的重要性优先级进行加密,简化了加密过程,而同一重要性优先级的数据可采用同一密码,因而,减少了密码数量,使得加密中使用的密码较容易记住。

[0097] 本发明实施例还提供一种计算机存储介质,其中,该计算机存储介质可存储有程序,该程序执行时包括上述方法实施例中记载的任意一种信号处理方法的部分或全部步骤。

[0098] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中未详述的部分,可以参见其他实施例的相关描述。

[0099] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可能可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0100] 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,可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,例如上述单元的划分,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,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性或其它的形式。

[0101] 上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0102] 另外,在本发明各实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0103] 上述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式

体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以为个人计算机、服务器或者网络设备等,具体可以是计算机设备中的处理器)执行本发明各个实施例上述方法的全部或部分步骤。其中,而前述的存储介质可包括:U盘、移动硬盘、磁碟、光盘、只读存储器(英文:Read-Only Memory,缩写:ROM)或者随机存取存储器(英文:Random Access Memory,缩写:RAM)等各种可以存储程序代码的介质。

[0104] 以上所述,以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

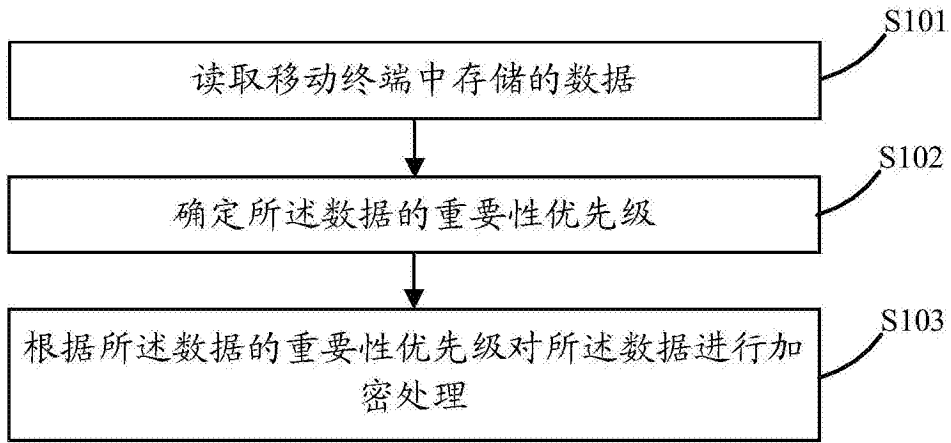


图 1

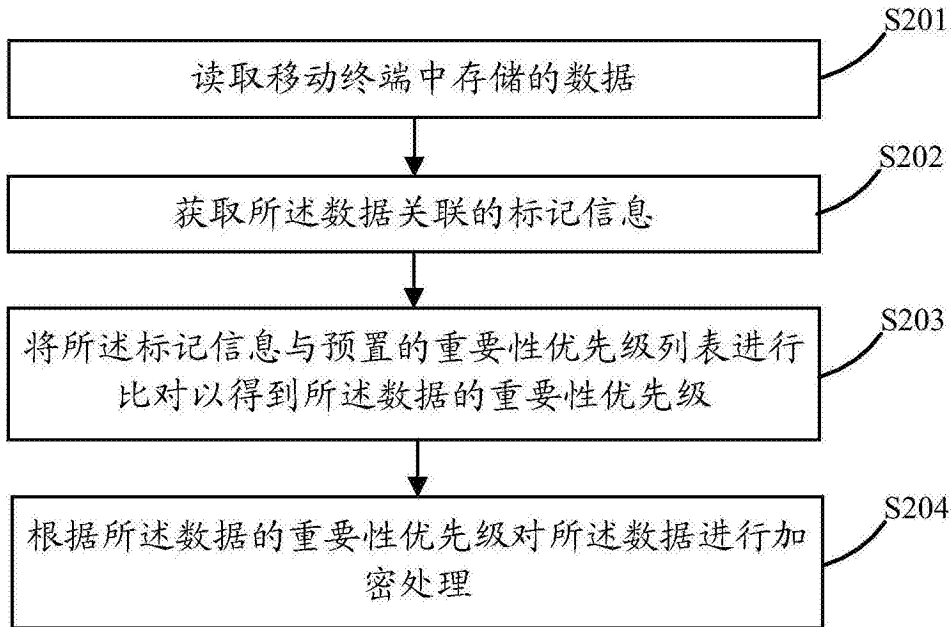


图 2

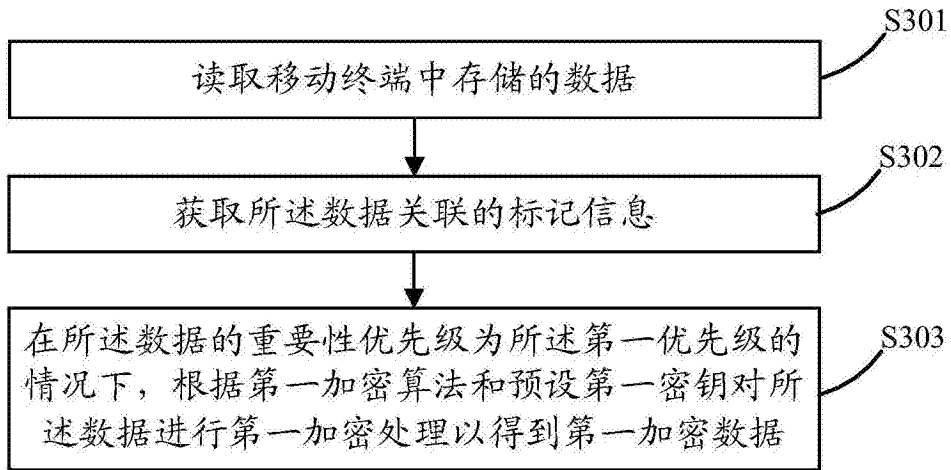


图 3

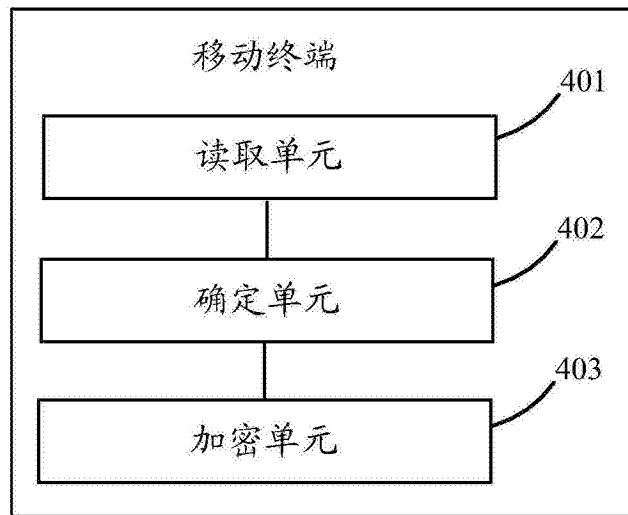


图 4a

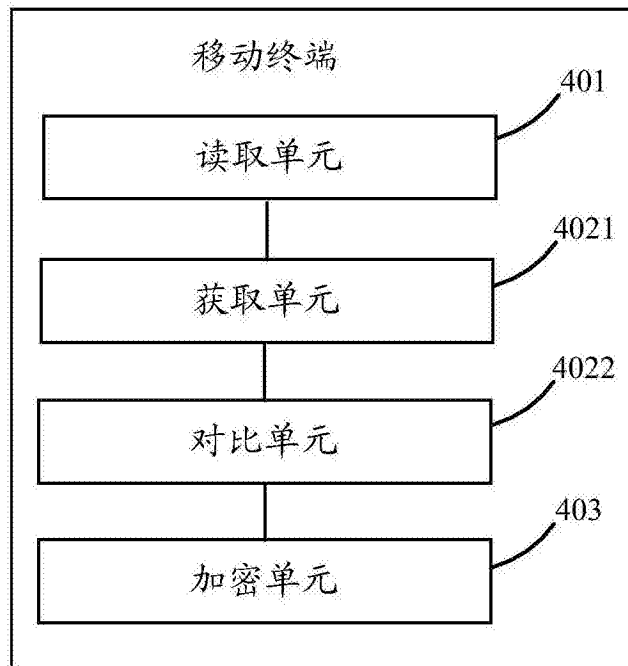


图 4b

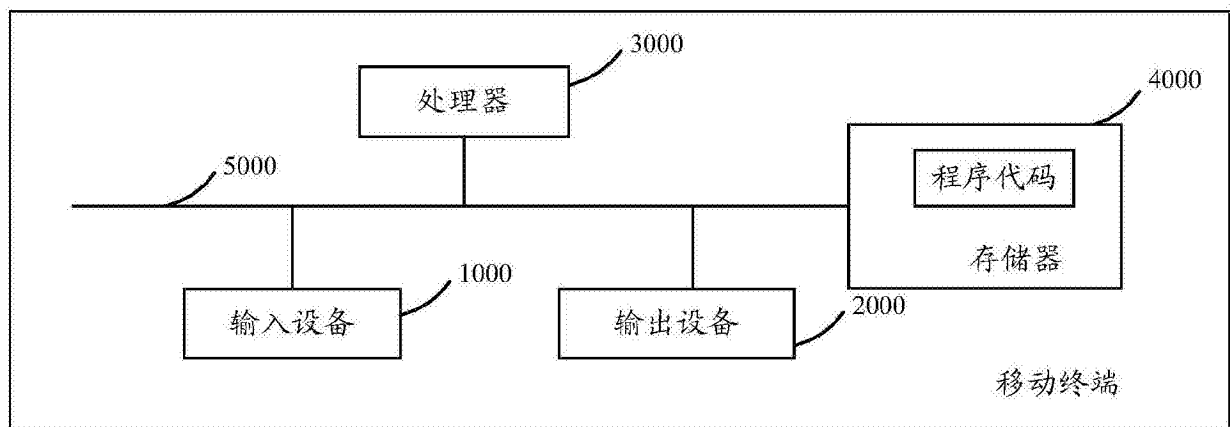


图 5