(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
2014 年 12 月 11 日 (11.12.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/194828 A1

(51) 国际专利分类号:
G06F 12/14 (2006.01)

(21) 国际申请号: PCT/CN2014/079167

(22) 国际申请日: 2014 年 6 月 4 日 (04.06.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310226540.7 2013 年 6 月 7 日 (07.06.2013) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **曹建峰 (CAO, Jianfeng)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **周晨光 (ZHOU, Chenguang)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **赵江 (ZHAO, Jiang)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京华沛德权律师事务所 (BEIJING BRIGHT & RIGHT LAW FIRM)**; 中国北京市朝阳区朝外大街乙 12 号昆泰国际大厦 1008 室, Beijing 100020 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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,

[见续页]

(54) **Title**: FILE ENCRYPTION/DECRYPTION METHOD AND FILE ENCRYPTION/DECRYPTION DEVICE

(54) **发明名称** : 一种文件加/解密方法以及文件加/解密装置

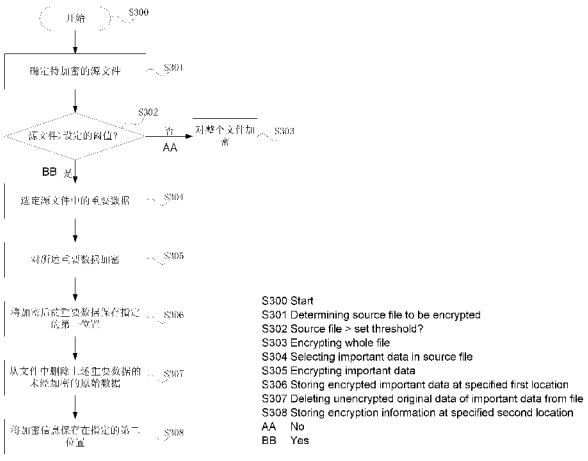

图 3/Fig. 3

(57) **Abstract**: Provided are a file encryption and decryption method and file encryption and decryption device. The encryption method comprises: determining the source file to be encrypted; selecting important data in the source file; encrypting the important data according to a pre-set encryption algorithm; storing the encrypted important data at a specified first location; deleting unencrypted important data from the source file; storing the encryption information at a specified second location, the encryption information at least including the original location of the important data in the source file. Also provided is a decryption method that corresponds to the encryption method, and an encryption and decryption device. The decryption difficulty is enhanced due to partial encryption, in which whether encrypted important data exists in the source file must be known during decryption, and the storage location of the encrypted data must be known.

(57) **摘要**:

[见续页]

WO 2014/194828 A1

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

提供了一种文件加密及解密方法以及加密及解密装置，所述加密方法包括：确定待加密的源文件；选定源文件中的重要数据；根据设定的加密算法对重要数据执行加密；在指定的第一位置，保存加密后的重要数据；从源文件中删除未加密的重要数据；将加密信息保存在指定的第二位置；加密信息至少包括所述重要数据在源文件中的原始位置；相对于该加密方法还提供了解密方法，以及加密及解密装置，由于实现局部加密，当解密时需要知道源文件中是否存在加密的重要数据，且需要知道该加密数据的存放位置，因此增加了解密的难度。

一种文件加/解密方法以及文件加/解密装置

技术领域

本发明涉及计算机应用技术领域，特别是涉及一种文件加密方法及与该文件加密方法相应的解密方法；本发明同时涉及一种文件加密装置及与该文件加密装置相应的解密装置。

背景技术

文件加密是一种根据要求在操作系统层对写入存储介质的数据进行加密的技术。

文件加密按加密途径可分为两类：一类是系统自带的文件加密功能；一类是采用加密算法实现的加密功能。

一般情况下，对数据加密是指通过加密算法和加密密钥将明文转变为密文，而解密则是通过解密算法和解密密钥将密文恢复为明文。具体地，对数据的保护是将数据所在的文件，按照某种算法进行处理，使该文件成为不可读的一段代码，只能在输入相应的密钥以后才能显示出文件本来内容，以到达保护文件数据不被非法窃取和阅读的目的。如图1和图2所示，都是通过向算法中输入密钥（Key），来实现对整个文件的加密与解密。

另外，随着人们对个人隐私的保护日渐重视，越来越多的人需要的对自己的私人文件进行保护，尤其是随着智能移动终端的盛行，该终端不在只是一个简单的通信工具，里面可能保存各种重要文件，当对该些重要文件进行加密时通常采用的方式是，先选定需要加密的文件或者文件夹，之后通过系统设定的加密按键进行加密，以保证数据信息的安全。

可以了解的是，上述的加密方法是对整个文件或文件夹加密，存储的文件或文件夹越大，对其加密所需要花费的时间就越长；相应地，对文件解密所花费的时间也会越长。当用户对文件加密处理方式在加密处理能力方面的性能要求较高，而所使用的设备的运算能力又比较低时--例如在移动终端中对其中拍摄的照片进行加密--则该种加密方式尤其不能满足用户的需求。在这种情况下，还要考虑到，当系统资源被大量用于需要占用大量运算能力的加密计算时，加密操作还会影响其它文件的运行，导致系统响应速度的整体降低。

如何提供一种文件加密及解密方法以及加密及解密装置，在有效实现用户对文件加密方式高性能要求的同时，又不至于影响系统的响应速度，成为亟待

解决的问题。

发明内容

为解决上述技术问题，本发明提供一种文件加密及解密方法以及加密及解密装置，能够符合用户对文件加密性能要求的同时，还提高了系统的响应速度。

本发明提供的一种文件加密方法，包括:

确定待加密的源文件;

选定源文件中的重要数据;

根据设定的加密算法对所述重要数据执行加密;

在指定的第一位置，保存加密后的所述重要数据;

从所述源文件中删除未加密的所述重要数据;

将加密信息保存在指定的第二位置;所述加密信息至少包括所述重要数据在源文件中的原始位置。

本发明同时提供一种文件解密方法，包括:

读取已加密的加密文件，该已加密的加密文件中，仅重要数据被加密;

从第一位置获取已加密重要数据;

通过第二位置读取加密信息，该加密信息至少包括所述重要数据源文件中的原始位置；；

根据加密信息执行解密，并将解密后的重要数据放在所述加密信息所提供的所述重要数据在源文件中的原始位置;

保存还原后的源文件。

本发明同时提供一种文件加密装置，包括:

选定器，用于选定待加密源文件中的重要数据;

加密器，用于接收所述选定器选定的重要数据，并根据设定的加密算法对所述重要数据加密;

加密数据保存器，用于接收所述加密器提供的加密后的重要数据，将上述加密后的重要数据保存在指定的第一位置;

删除器，用于将源文件中未加密的所述重要数据删除;

加密信息生成保存器，用于根据上述加密过程生成加密信息，并将该加密信息保存在所述指定第二位置，所述加密信息至少包括所述重要数据在源文件中的原始位置。

本发明同时提供一种文件解密装置，包括:

加密文件读取器，读取已加密文件，且该已加密的文件中仅重要数据被加密;

加密信息读取器，从指定位置读取加密信息，该加密信息至少包括重要数据在未加密的源文件中的原始位置；

加密数据读取器，从指定位置读取所述已加密文件内的重要数据；

解密器，用于接收所述加密数据读取器读取的重要数据，并使用对应所述加密后重要数据的加密算法的解密算法，对所述加密后的重要数据解密；

解密数据回放器，用于接收所述加密信息读取器读取的加密信息，并根据加密信息中的提供的重要数据在未加密的源文件中的原始位置，将解密后的重要数据放回所述原始位置。

根据本发明提供的一种文件加密及解密方法以及加密及解密装置的具体实现方法，本发明公开了以下技术效果：本发明通过选定文件中的重要数据，对所述确定的重要数据加密，使得加密操作仅针对于用户选定文件中重要数据实现局部加密，而不是对整个文件或文件夹加密，当解密时需要知道源文件中是否存在加密的重要数据，且需要知道该加密数据的存放位置，因此增加了解密的难度。另外，本发明仅是针对文件中重要数据部分加密，使需要加密的数据大幅度减少，可以明显提高加密速度和加密效率，减少设备加密运算量，使数据处理能力较低的设备—例如移动终端--可以快速执行加密处理。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术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中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

图1是现有技术中文件加密方法的示意图；

图2是现有技术中文件解密方法的示意图；

图3是本发明提供的一种文件加密方法实施例的流程图；

图4是本发明提供的一种文件解密方法实施例的流程图；

图5是本发明提供的一种文件加密装置实施例的框图；

图6是本发明提供的一种文件解密装置实施例的框图；

图7示出了用于执行根据本发明的方法的智能电子设备的框图；以及

图8示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元示意图。

具体实施方式

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一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本发明保护的范围。

请参阅图3，其为本发明提供的一种文件加密方法实施例的流程图。在本实施例中，包括如下步骤：

步骤S300是开始。

步骤S301是确定待加密的源文件。

该确定待加密的源文件可以是根据文件自身的重要性来确定，或者根据用户对文件重要性的要求来确定。

步骤S302是判断文件的大小是否大于设定的阈值。

在此步骤中，当确定待加密的源文件后，可以通过预先设定的阈值，与源文件大小比对，根据比对结果执行不同的操作，该阈值可以是文件或文件夹占用内存容量的容量值。当所述文件的大小小于预先设定的阈值，则进入步骤S303。

步骤S303是直接执行对整个文件加密，无需对文件中某一部分的数据加密，因为，由于文件所占内存的空间较小，对其加密的时间花费的也少，所以无需再通过选定文件重要数据来加密。反之，如果文件的大小大于预先设定的阈值，则进入步骤S304，步骤S304执行选定文件中的重要数据的步骤，有针对性的对选定文件中的重要数据加密，进而节省加密和解密的时间。

步骤S304：选定源文件中的重要数据；

在具体实现本步骤的过程中，重要数据可以是涉及系统文件内的数据；或者是用户选定的财务文件、生产文件、销售文件、市场文件、人力资源文件等内的数据；重要数据还可以是用户个人文件的数据，例如：照片、视频、日志等等。重要数据的选定方法可以有多种方式实现，下面仅给出几种具体实现方式的示例，用以对本发明步骤S304的说明。

（一）选定源文件中的重要数据的第一具体实现方式：

所述选定文件中的重要数据的方法，是识别文件类型，并根据文件类型选定重要数据位于该文件的固定位置。文件类型也称之为文件格式，常用的有JPG，PNG，EXE，COM，BMP，GIF，WMV，APE，RMVB，FLV，SWF，TXT，CPP，ASM等等。文件中包含有代码和数据等信息，该些信息是按段保存在文件头部，文件头部用来描述文件的总体结构。比如：EXE文件，其头部文件一般包括代码段、数据段、堆栈段和扩展段等等，代码段存放了计算机的执行指令，即CPU要进行的操作指令；数据段存放了CPU要用到的数据；堆栈段则存放了与寄存

器有关的信息等等。JPG文件中的头部信息用来解析JPG，而对于解析JPG的数据长度可变，对其加密后，其他图片浏览器将无法正常读取。PNG文件同样也是通过文件头保护文件重要信息，而该文件头的重要信息数据长度固定，对其加密后，其他图片浏览器也将不能正常读取。当确定了文件类型之后，根据该文件的文件头部来选定重要数据位于该文件的固定位置，之后根据所述固定位置对该些重要数据加密。

（二）选定源文件中的重要数据的第二具体实现方式：

所述选定文件中的重要数据的方法，是接收用户对文件重要数据的指定。若所述文件为文本文件，则用户可以将文本文件中的某页或某个段落指定为重要数据，通过指定的页码对该页内容加密或通过指定段落的初始位置和结束位置计算出段落的区域，并通过调用提取函数，提取出用户指定的重要数据，并对提取的重要数据加密。如果所述文件为图形文件，则用户可以将选取图形文件中图形的某一处或多处的重要部分，通过调用截屏函数，对截取后的重要数据加密。

步骤S305：根据设定的加密算法对所述重要数据加密；

对提取出的重要数据加密，加密方法可以通过设定的密钥，采用加密算法，对重要数据加密，实际上在加密的方式可以有多种，在此不再赘述。

步骤S306：将上述加密后的重要数据保存在指定的第一位置；

重要数据加密后，将其保存在指定的第一位置，该第一位置可以是所述源文件中指定位置，或另一个文件的指定位置，该指定位置可以是在本体端或者在服务器端。也就是说，指定的位置可以是任意位置，且第一位置和第二位置可能重合。

步骤S307：从文件中删除上述重要数据的未经加密的原始数据；

在保存加密的重要数据后，将文件中原始的重要数据删除，从而使得在打开原始文件时，其中重要数据部分为不可见，避免了重要数据的泄露。

步骤S308：将加密信息保存在指定的第二位置，该加密信息至少包括加密后重要数据的原始位置。所述加密信息保存的指定的第二位置可以为源文件头部。

另外，还可以将加密后的所述重要数据与所述源文件中重要数据以外的数据一起封装为加密文件，并以所述加密文件替换所述源文件；或者，仅将所述加密后重要数据以外的数据封装为未加密文件，并以所述未加密文件替换所述源文件。

由于本发明提供的加密方法是通过选定源文件中重要数据部分，进行重要数据部分加密，即：局部加密，使得该方法比全部源文件采用统一的加密方式

具有更好的加密效果，因为，当解密时需要知道源文件中是否存在加密的重要数据，且需要知道该加密数据的存放位置，因此增加了解密的难度；另外，本发明仅是针对文件中重要数据部分加密，提高加密效率、并且对于数据处理能力较低的设备可以实现快速执行加密处理的功能。

以上公开了本发明一种文件加密方法的实施例，与所述加密方法实施例相对应，本发明还公开了一种用于文件解密方法的实施例，请参看图4，图4为本发明一种文件解密方法实施例流程图。

步骤S400是开始解密；

步骤S401是读取已加密的加密文件，该已加密的加密文件中，仅重要数据被加密；

步骤S402是从第一位置获取已加密重要数据；

步骤S403是通过第二位置读取加密信息，该加密信息至少包括所述重要数据源文件中的原始位置；

步骤S404是根据读取的加密信息执行解密，并将解密后的重要数据放在所述加密信息所提供的所述重要数据在源文件中的原始位置；

步骤S405是保存还原后的源文件。

上述步骤是根据加密方法中在文件指定的第二位置存储的加密信息实现，该第二位置可以是所述源文件的指定位置，例如：源文件头部。或者是另一文件的指定位置，所述的指定位置可以是在本地端或者在服务器端。如果是在源文件头部，解密时通过读取文件头部信息，获取重要数据的保存位置、重要数据的原始位置和加密方法等信息，实现解密，获得重要数据的具体内容。

当上述加密方法应用在Android平台时，用户可以将经上述方法加密后的文件备份在Android系统的固定位置，例如：隐私保险箱。文件放入之后，该隐私保险箱会将该文件原有的文件格式破坏，用户只有通过预先设定的验证密码登陆隐私保险箱后，才能正常打开加密文件。如果不是通过隐私保险箱的方式查找加密文件，即使查找到也无法从文件中找到加密的重要数据并破解该重要数据的内容。

上述为本发明提供的一种文件加密及解密方法的具体实现方法，通过上述可以看出，本发明提供的文件加密及解密方法，并非对整个文件或文件夹加密；而是通过选定文件中的重要数据，对所述确定的重要数据加密，使得加密操作仅针对于用户选定文件中重要数据实现局部加密，而不是对整个文件或文件夹加密，当解密时需要知道源文件中是否存在加密的重要数据，且需要知道该加密数据的存放位置，因此增加了解密的难度。另外，本发明仅是针对文件中重要数据部分加密，提高加密效率、并且对于数据处理能力较低的设备可以实现

快速执行加密处理的功能。

通过上述公开的本发明一种文件加密及解密方法的实施例，与所述方法实施例相对应的，本发明还公开了一种文件加密及解密装置实施例，请参看图5，图5是本发明提供的一种文件加密装置实施例的框图。由于该加密装置实施例基本相似于加密方法的实施例，所以描述得比较简单，相关之处参见加密方法实施例的部分说明即可。下述描述的加密装置实施例仅仅是示意性的。

所述加密装置实施例包括:

选定器501，用于选定待加密源文件中的重要数据；加密器502，用于接收所述选定器选定的重要数据，并根据设定的加密算法对所述重要数据加密；加密数据保存器503，用于接收所述加密器提供的加密后的重要数据，将上述加密后的重要数据保存在指定的第一位置；删除器504，用于将源文件中未加密的所述重要数据删除；加密信息生成保存器505，用于根据上述加密过程生成加密信息，并将该加密信息保存在所述指定第二位置，所述加密信息至少包括所述重要数据在源文件中的原始位置。

另外，包括封装器506用于接收解密后的所述重要数据以及源文件中所述重要数据以外的数据，并将它们一起封装为解密后文件，并以该解密后的文件替换所述源文件；或者将所述解密后重要数据以外的数据封装为未解密文件，并以所述未解密文件替换所述源文件。

选定器501有多种具体实施方式，下面示意性的给出两种，这两种具体实施方式可以单独使用，也可以结合使用。

第一种方式是：所述选定器包括，文件类型识别子单元，用于识别文件类型并输出；选定执行子单元，用于接收所述文件类型，并根据文件类型选定重要数据所位于该文件的固定位置。

第二种方式是：所述选定器包括，指定单元，接收用户对文件重要数据的指定，并据此选定文件中的重要数据。

可选的，该装置进一步包括：文件大小判断单元，用于判断文件的大小是否大于预订的阈值，若是，则向所述选定器发送选定启动指令，所述选定器接收该选定启动指令后，启动对文件中的重要数据进行选定的过程；若否，则向加密器发出整体加密指令，所述加密器接收到该整体加密指令后，对整个文件进行加密。

请参看图6，图6是本发明提供的一种文件解密装置实施例的框图。

所述解密装置实施例包括:

加密文件读取器601，读取已加密文件，且该已加密的文件中仅重要数据被加密;

加密信息读取器602，从指定位置读取加密信息，该加密信息至少包括重要数据在未加密的源文件中的原始位置；

加密数据读取器603，从指定位置读取所述已加密文件内的重要数据；

解密器604，用于接收所述加密数据读取器读取的重要数据，并使用对应所述加密后重要数据的加密算法的解密算法，对所述加密后的重要数据解密；

解密数据回放器605，用于接收所述加密信息读取器读取的加密信息，并根据加密信息中的提供的重要数据在未加密的源文件中的原始位置，将解密后的重要数据放回所述原始位置。

以上对本发明所提供的文件加密及解密方法以及加密及解密装置进行了详细介绍，本文中应用了具体各例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处。综上所述，本说明书内容不应理解为对本发明的限制。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的移动终端处理可视化图形编码中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图7示出了可以实现根据本发明的文件加密方法及与该文件加密的方法的智能电子设备。该智能电子设备传统上包括处理器710和以存储器720形式的计算机程序产品或者计算机可读介质。存储器720可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者ROM之类的电子存储器。存储器720具有用于执行上述方法中的任何方法步骤的程序代码731的存储空间730。例如，用于程序代码的存储空间730可以包括分别用于实现上面的方法中的各种步骤的各个程序代码731。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图8所述的便携式或者固定存储单元。该存储单元可以具有与图7的智能电子设备中的存储器720类似布置的存储段或者存储空间等。程序代码可以例如以

适当形式进行压缩。通常，存储单元包括用于执行根据本发明的方法步骤的程序731'，即可以由例如诸如710之类的处理器读取的代码，这些代码当由智能电子设备运行时，导致该智能电子设备执行上面所描述的方法中的各个步骤。

5

权 利 要 求

1、一种文件加密方法，其特征在于，包括:

确定待加密的源文件;

选定源文件中的重要数据;

根据设定的加密算法对所述重要数据执行加密;

在指定的第一位置，保存加密后的所述重要数据;

从所述源文件中删除未加密的所述重要数据;

将加密信息保存在指定的第二位置;所述加密信息至少包括所述重要数据在源文件中的原始位置。

2、根据权利要求1所述的文件加密方法，其特征在于，包括:将加密后的所述重要数据与所述源文件中重要数据以外的数据一起封装为加密文件，并以所述加密文件替换所述源文件。

3、根据权利要求1所述的文件加密方法，其特征在于，包括:将所述加密后重要数据以外的数据封装为未加密文件，并以所述未加密文件替换所述源文件。

4、根据权利要求1所述的文件加密方法，其特征在于，所述加密信息包括:所述重要数据在源文件中的存储空间和/或存储位置和/或加/解密算法。

5、根据权利要求1所述的文件加密方法，所述第一位置和第二位置是所述源文件的指定位置，或另一个文件的指定位置，该指定位置是本地或服务器;所述本地为移动终端或者其它计算设备。

6、根据权利要求1所述的文件加密方法，所述重要数据为影响源文件正常打开的数据、和/或用户指定的数据、和/或源文件中实质内容的全部或部分数据。

7、根据权利要求1所述的文件加密方法，所述选定源文件重要数据为用户指定的数据时;此种情况下，若所述源文件为文本文件，则为用户指定的文本中重要段落;若所述源文件为图形文件，则为用户指定的图形中重要区域。

8、根据权利要求1所述的文件加密方法，所述选定源文件中的重要数据，其方法为:识别源文件的文件类型，并根据文件类型获取所述重要数据在源文件中的原始位置。

9、根据权利要求1所述的文件加密方法，首先判断所述源文件的大小是否大于设定的阈值，若是，则进入选定源文件中的重要数据的步骤;若否，则直接将源文件的所有数据作为所述重要数据。

10、一种文件解密方法，其特征在于，包括:

读取已加密的加密文件，该已加密的加密文件中，仅重要数据被加密;

从第一位置获取已加密重要数据;

通过第二位置读取加密信息,该加密信息至少包括所述重要数据源文件中的原始位置;

根据加密信息执行解密,并将解密后的重要数据放在所述加密信息所提供的所述重要数据在源文件中的原始位置;

保存还原后的源文件。

11、根据权利要求10所述的解密方法,识别文件的类型,并根据文件类型获取所述加密文件的第一位置。

12、一种文件加密装置,其特征在于,包括:

选定器,用于选定待加密源文件中的重要数据;

加密器,用于接收所述选定器选定的重要数据,并根据设定的加密算法对所述重要数据加密;

加密数据保存器,用于接收所述加密器提供的加密后的重要数据,将上述加密后的重要数据保存在指定的第一位置;

删除器,用于将源文件中未加密的所述重要数据删除;

加密信息生成保存器,用于根据上述加密过程生成加密信息,并将该加密信息保存在所述指定第二位置,所述加密信息至少包括所述重要数据在源文件中的原始位置。

13、根据权利要求12所述的文件加密装置,其特征在于,包括:

封装器,用于接收解密后的所述重要数据以及源文件中所述重要数据以外的数据,并将它们一起封装为解密文件,并以该解密文件替换所述源文件;或者将所述解密后重要数据以外的数据封装为未解密文件,并以所述未解密文件替换所述源文件。

14、根据权利要求12所述的文件加密装置,其特征在于,所述选定器包括:

文件类型识别子单元,用于识别源文件类型并输出;

选定执行子单元,用于接收所述源文件类型,并根据所述文件类型选定重要数据所位于该源文件的原始位置和/或重要数据的加密算法。

15、根据权利要求12所述的文件加密装置,其特征在于,所述选定器包括:

文件类型识别子单元,用于识别源文件类型并输出;

指定单元,接收用户根据所述文件类型对源文件中重要数据的指定,并据此选定源文件中的重要数据。

16、根据权利要求12所述的文件加密装置,包括判断单元,用于判断文件的大小是否大于设定的阈值,若是,则向所述选定器发送选定启动指令,所述选定器接收该选定启动指令后,启动对文件中的重要数据进行选定的过程;若

否，则向加密器发出整体加密指令，所述加密器接收到该整体加密指令后，对整个文件进行加密。

17、一种文件解密装置，其特征在于，包括:

加密文件读取器，读取已加密文件，且该已加密的文件中仅重要数据被加密;

加密信息读取器，从指定位置读取加密信息，该加密信息至少包括重要数据在未加密的源文件中的原始位置;

加密数据读取器，从指定位置读取所述已加密文件内的重要数据;

解密器，用于接收所述加密数据读取器读取的重要数据，并使用对应所述加密后重要数据的加密算法的解密算法，对所述加密后的重要数据解密;

解密数据回放器，用于接收所述加密信息读取器读取的加密信息，并根据加密信息中的提供的重要数据在未加密的源文件中的原始位置，将解密后的重要数据放回所述原始位置。

18、一种计算机程序，包括计算机可读代码，当智能电子设备运行所述计算机可读代码运行时，导致权利要求1-11中的任一项权利要求所述的方法被执行。

19、一种计算机可读介质，其中存储了如权利要求18所述的计算机程序。

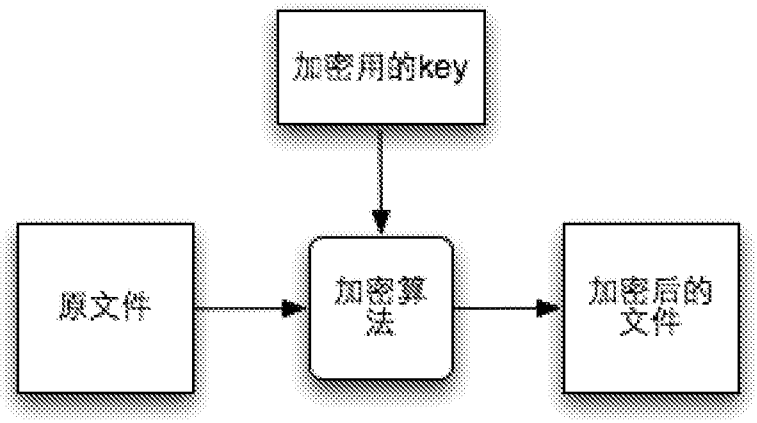

图 1

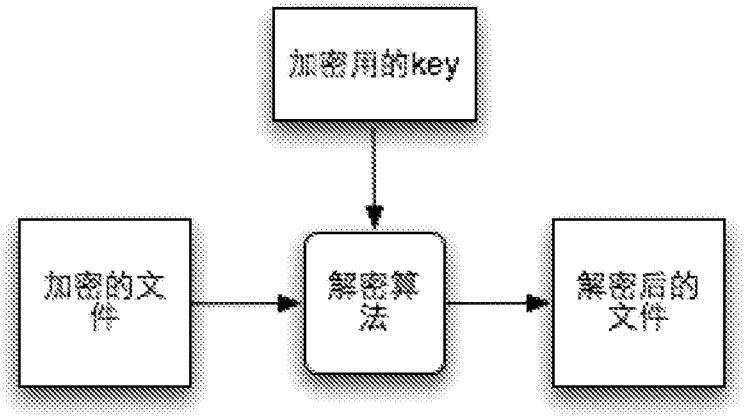

图 2

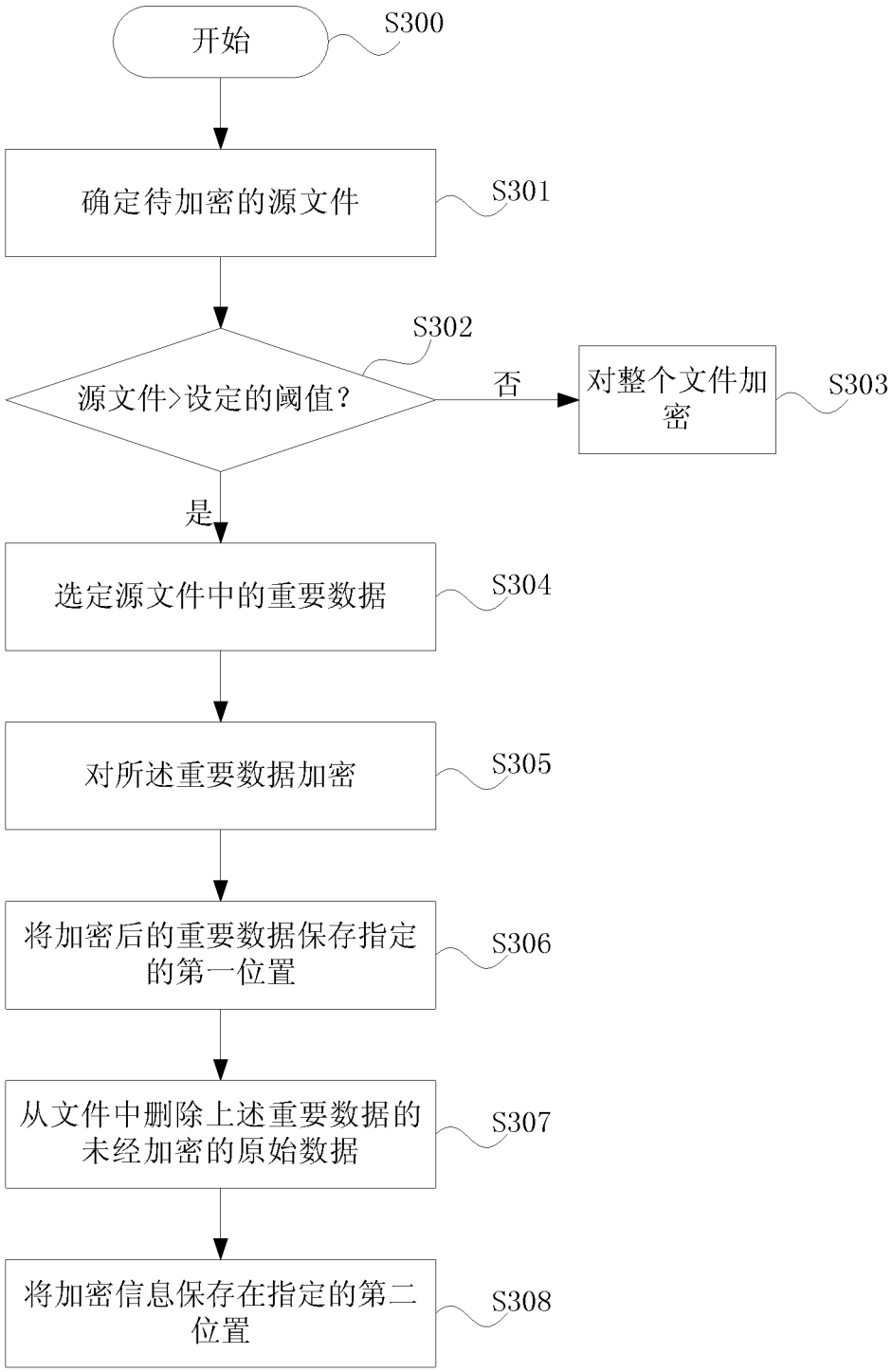
开始
S300
确定待加密的源文件
S301
S302
源文件>设定的阈值？
否
对整个文件加密
S303
是
选定源文件中的重要数据
S304
对所述重要数据加密
S305
将加密后的重要数据保存指定的第一位置
S306
从文件中删除上述重要数据的未经加密的原始数据
S307
将加密信息保存在指定的第二位置
S308

图 3

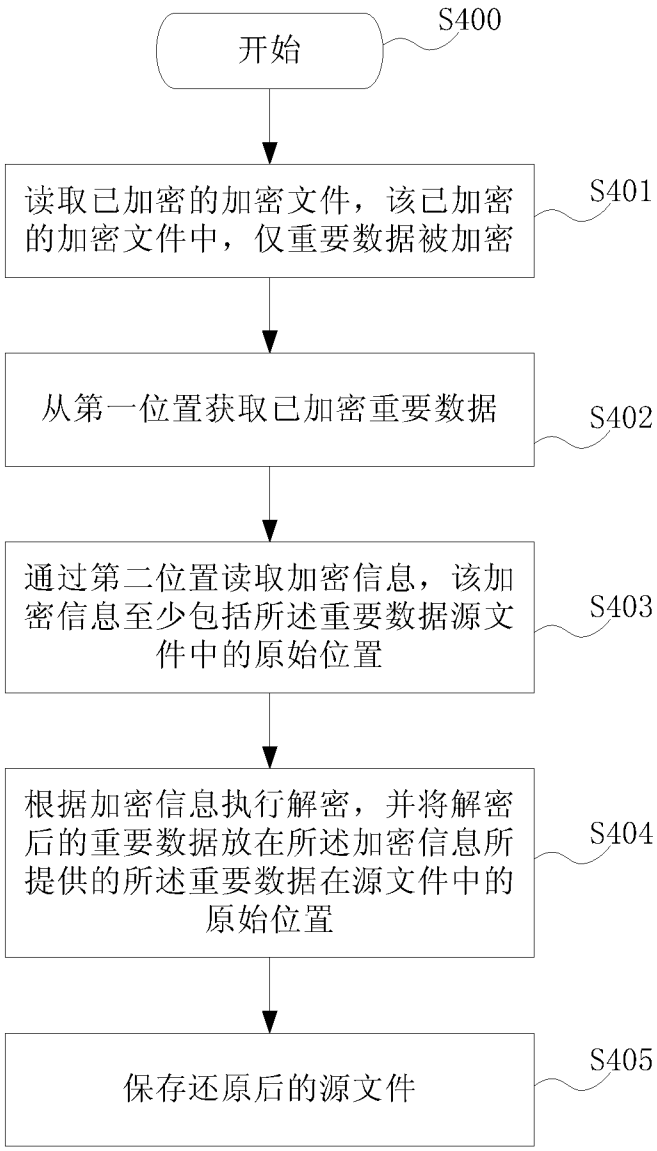
开始
S400
读取已加密的加密文件，该已加密的加密文件中，仅重要数据被加密
S401
从第一位置获取已加密重要数据
S402
通过第二位置读取加密信息，该加密信息至少包括所述重要数据源文件中的原始位置
S403
根据加密信息执行解密，并将解密后的重要数据放在所述加密信息所提供的所述重要数据在源文件中的原始位置
S404
保存还原后的源文件
S405

图 4

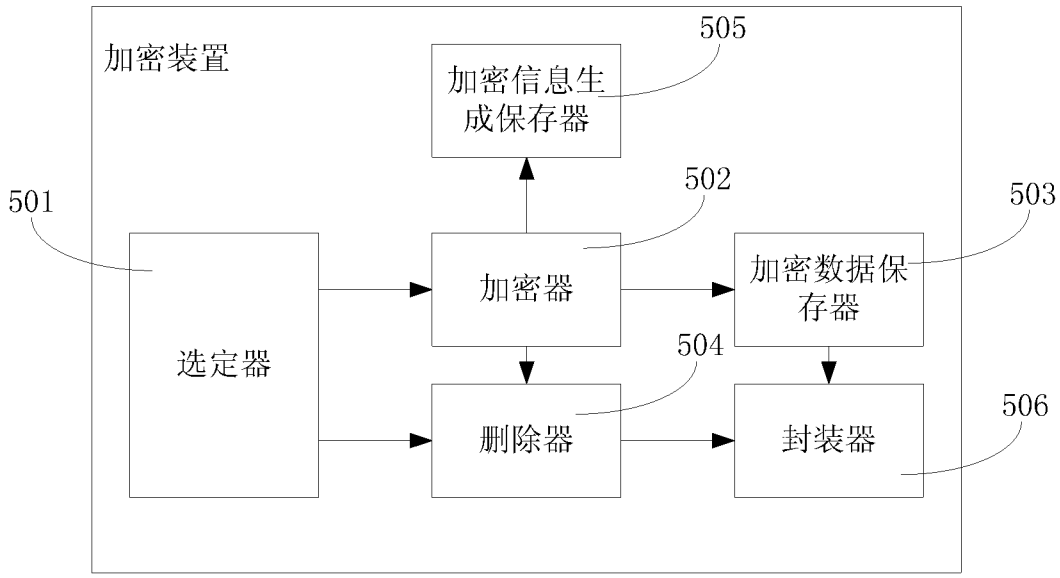
加密装置
505
加密信息生成保存器
501
502
503
选定器
加密器
加密数据保存器
504
506
删除器
封装器

图 5

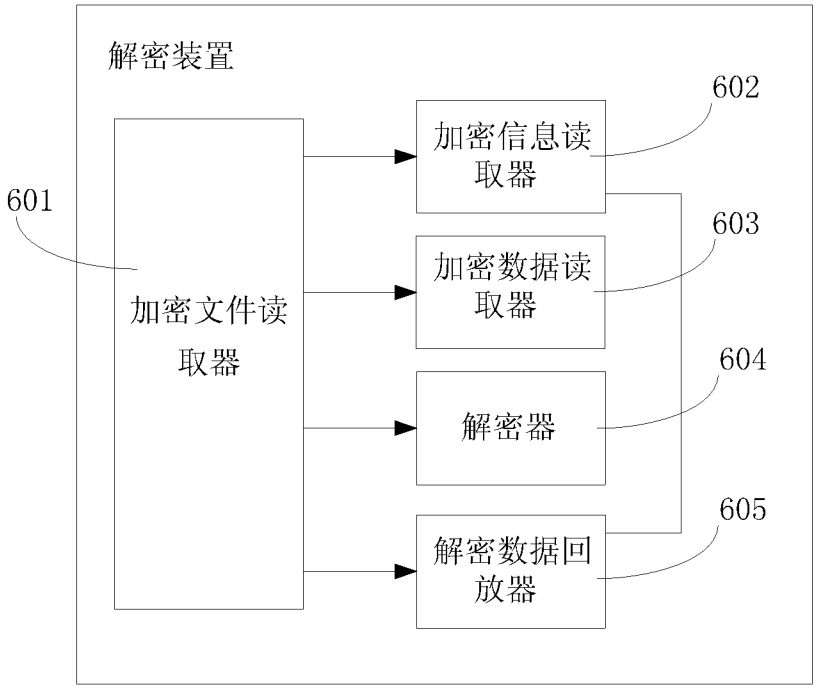
解密装置
602
601
加密信息读取器
603
加密文件读取器
加密数据读取器
604
解密器
605
解密数据回放器

图 6

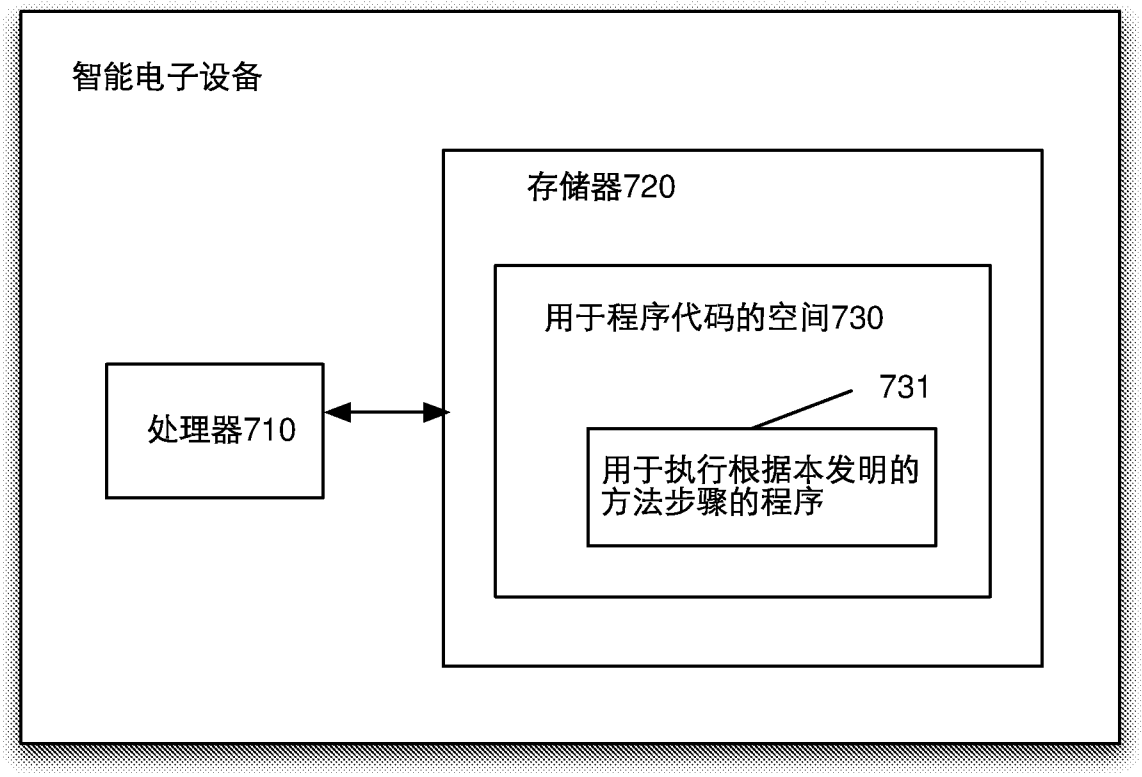
智能电子设备
存储器720
用于程序代码的空间730
731
处理器710
用于执行根据本发明的方法步骤的程序

图 7

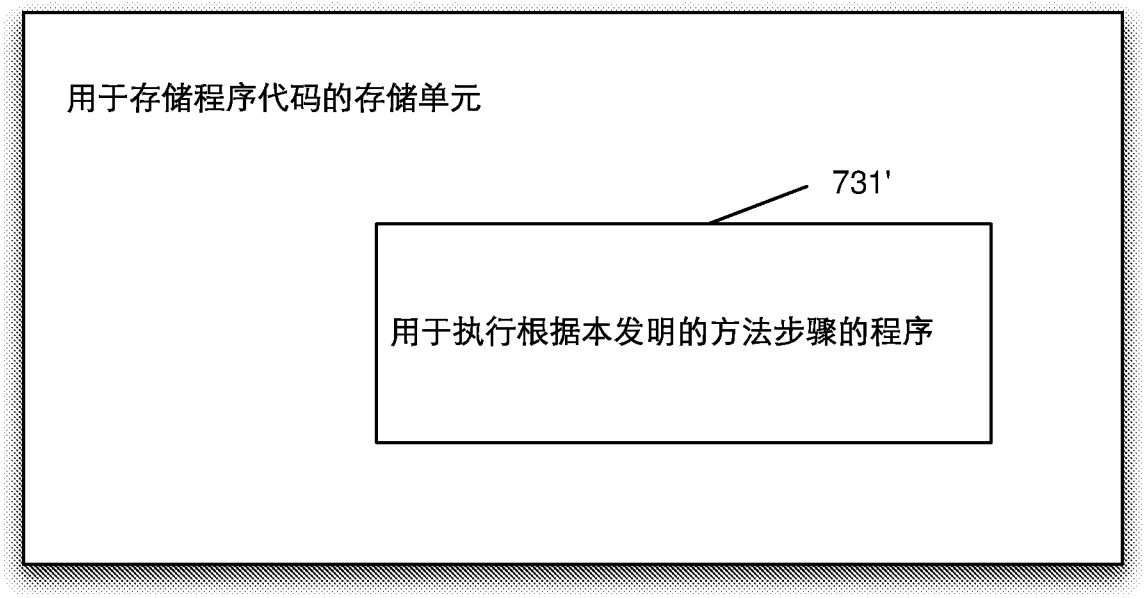
用于存储程序代码的存储单元
731'
用于执行根据本发明的方法步骤的程序

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/079167

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/14 (2006.01) 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, EPODOC, WPI: decrypt, delete, ENCRYPT, IMPORT+, SAVE, POSITION, LOCA+, DOCUMENT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103294961 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 11 September 2013 (11.09.2013), description, paragraphs [0008]-[0151]	1-19
X	CN 101667162 A (INVENTEC CORPORATION), 10 March 2010 (10.03.2010), claims 1, 5 and 9, and description, page 3, line 14 to page 4, line 8, and page 4, line 13 to page 5, line 19	1-19
A	CN 102456116 A (JIANGNAN INSTITUTE OF COMPUTING TECHNOLOGY), 16 May 2012 (16.05.2012), the whole document	1-19
A	CN 102254127 A (HUAWEI TECHNOLOGIES CO., LTD.), 23 November 2011 (23.11.2011), the whole document	1-19

☐ 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
19 August 2014 (19.08.2014)	**22 September 2014 (22.09.2014)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **WANG, Ning** Telephone No.: (86-10) **62414033**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/079167

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103294961 A	11 September 2013	None	
CN 101667162 A	10 March 2010	None	
CN 102456116 A	16 May 2012	None	
CN 102254127 A	23 November 2011	WO 2013020446 A1	14 February 2013

国际检索报告

国际申请号 PCT/CN2014/079167

A. 主题的分类

G06F 12/14(2006.01)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,EPODOC,WPI: 加密，解密，重要，保存，位置，删除，ENCRYPT, IMPORT+, SAVE, POSITION, LOCA+, DOCUMENT

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 103294961 A (北京奇虎科技有限公司 等) 2013年 9月 11日 (2013 - 09 - 11) 说明书第[0008]-[0151]段	1-19
X	CN 101667162 A (英业达股份有限公司) 2010年 3月 10日 (2010 - 03 - 10) 权利要求1，5，9，说明书第3页第14行-第4页第8行，第4页第13行-第5页第19行	1-19
A	CN 102456116 A (无锡江南计算技术研究所) 2012年 5月 16日 (2012 - 05 - 16) 全文	1-19
A	CN 102254127 A (华为技术有限公司) 2011年 11月 23日 (2011 - 11 - 23) 全文	1-19

☐ 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
2014年 8月 19日	2014年 9月 22日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	王宁 电话号码 (86-10)62414033

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/079167

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 103294961 A	2013年 9月 11日	无	
CN 101667162 A	2010年 3月 10日	无	
CN 102456116 A	2012年 5月 16日	无	
CN 102254127 A	2011年 11月 23日	WO 2013020446 A1	2013年 2月 14日