(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
2017 年 10 月 5 日 (05.10.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/167052 A1

(51) 国际专利分类号:
G06F 21/62 (2013.01)

(21) 国际申请号: PCT/CN2017/077279

(22) 国际申请日: 2017 年 3 月 20 日 (20.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610188604.2 2016 年 3 月 29 日 (29.03.2016) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人; 及
(71) 申请人 (仅对美国): 吕晨晨 (LV, Chenchen) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 管维刚 (GUAN, Weigang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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)。

[见续页]

(54) Title: METHOD AND DEVICE FOR CONCEALING USER INFORMATION CONTAINED IN APPLICATION

(54) 发明名称 : 基于应用程序的用户信息的隐藏方法及装置

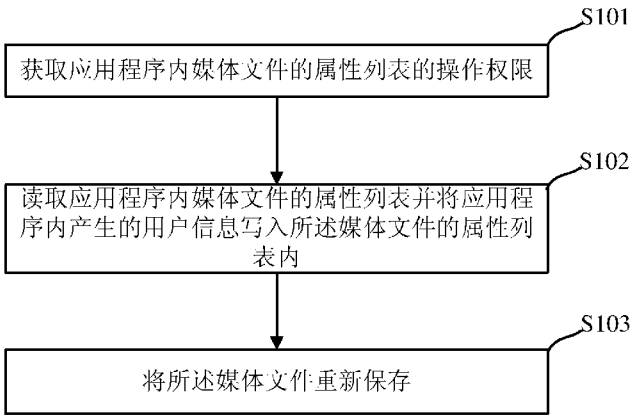

图 1

S101 ACQUIRE OPERATIONAL AUTHORIZATION FOR AN ATTRIBUTE LIST OF A MEDIA FILE IN AN APPLICATION

S102 READ THE ATTRIBUTE LIST OF THE MEDIA FILE IN THE APPLICATION PROGRAM AND WRITE USER INFORMATION GENERATED IN THE APPLICATION INTO THE ATTRIBUTE LIST OF THE MEDIA FILE

S103 RESAVE THE MEDIA FILE

(57) Abstract: Disclosed in the present invention are a method and a device for concealing user information contained in an application. The method comprises: acquiring operational authorization for an attribute list of a media file in an application; reading the attribute list of the media file in the application and writing user information generated in the application into the attribute list of the media file; resaving the media file. By writing user information generated in an application into an attribute list of a media file in the application, the present invention enables user information to be concealed, such that the user information cannot be easily found and acquired from a local folder of a mobile terminal, preventing user information generated through use of the application from being leaked.

(57) 摘要: 本申请公开了一种基于应用程序的用户信息的隐藏方法及装置。该方法包括：获取应用程序内媒体文件的属性列表的操作权限；读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内；将所述媒体文件重新保存。通过将应用程序内产生的用户信息写入应用程序的媒体文件的属性列表内，如此用户信息得到隐藏，在移动终端本地文件夹内不易被找到和获取，从而达到防止产生应用程序内的用户信息被泄露目的。

WO 2017/167052 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

基于应用程序的用户信息的隐藏方法及装置

技术领域

本申请涉及终端技术领域，尤其涉及一种基于应用程序的用户信息的隐藏方法及装置。

背景技术

在各种无线移动终端以及移动互联网飞速发展的时境下，越来越多的无线移动终端被应用于人们的日常生活中，很多无线移动终端已发展成为生活中的一部分。目前不论是 iOS、Android 还是 Windows 系统，数据传播的快速性、方便性、稳定性和安全性已经成为衡量一个无线移动终端的重要指标，尤其在涉及到用户重要、私有信息时，安全性更是重中之重。

在无线移动终端中使用应用程序可以实现购物、聊天、交友、出行等各种生活、工作功能，极大地方便用户。使用应用程序过程中，应用程序会生成各种数据，如应用程序登录的帐号、密码，以及如聊天记录、购物的订单信息、支付信息等涉及敏感、机密的用户信息。这些用户信息一般以文本文件及数据库文件的形式保存于移动终端本地文件夹内，因此，上述文本文件及数据库文件容易被查找到从而容易导致用户信息的泄露。为了防止用户信息轻易泄露，应用程序运行中生成的敏感、机密的用户信息会预先进行加密后再存储在移动终端本地文件夹内。然而，虽然上述信息已经被加密，但是加密的信息密文串还是完全暴露在外边，比如，可以通过目前比较常见的第三方工具（itools、豌豆荚等数据库工具）查到文本文件及数据库文件（如.txt、.db、.plist 等文件），从而获取这些加密后的信息，这样增加了对敏感、机密信息被破解概率，导致敏感、机密的用户信息泄露，安全性较低。

发明内容

本申请实施例提供一种基于应用程序的用户信息的隐藏方法及装置，用以解决现有技术中在应用程序运行过程中产生的用户信息容易被发现和获取，而导致用户信息泄露的问题。

本申请实施例提供一种基于应用程序的用户信息的隐藏方法，其包括:

获取应用程序内媒体文件的属性列表的操作权限;

读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内;

将所述媒体文件重新保存。

进一步的，所述用户信息包括敏感或机密的信息。

进一步的，所述获取应用程序内媒体文件的属性列表的操作权限，具体包括:

获取应用程序内媒体文件的句柄;

通过媒体文件的句柄，来获取应用程序内媒体文件的属性列表的读取、写入权限。

进一步的，所述将应用程序内产生的用户信息写入所述媒体文件的属性列表内，具体包括:

将应用程序内产生的用户信息以键值对的形式写入所述媒体文件的属性列表内。

进一步的，所述媒体文件包括照片、音频及视频文件。

进一步的，所述用户信息为加密过的用户信息。

本申请实施例还提供了一种基于应用程序的用户信息的隐藏方法，其包括:

获取应用程序内媒体文件的属性列表的操作权限;

对应用程序内产生的用户信息进行逻辑处理;

读取应用程序内媒体文件的属性列表并将应用程序内经过逻辑处理的用户信息写入所述媒体文件的属性列表内;

将所述媒体文件重新保存。

进一步的，所述用户信息包括敏感或机密的信息。

进一步的，所述获取应用程序内媒体文件的属性列表的操作权限，具体包括:

获取应用程序内媒体文件的句柄;

通过媒体文件的句柄，来获取应用程序内媒体文件的属性列表的读取、写入权限。

进一步的，所述将应用程序内产生的用户信息写入所述媒体文件的属性列表内，具体包括:

将应用程序内产生的用户信息以键值对的形式写入所述媒体文件的属性列表内。

进一步的，所述媒体文件包括照片、音频及视频文件。

进一步的，所述用户信息为加密过的用户信息。

进一步的，所述对应用程序内产生的用户信息进行逻辑处理，具体包括:

对应用程序内产生的用户信息进行可逆的逻辑处理。

进一步的，所述对应用程序内产生的用户信息进行逻辑处理，具体包

括:

通过对称加密算法，对应用程序内产生的用户信息进行对称加密处理。

本申请实施例还提供了一种基于应用程序的用户信息的隐藏装置，其包括:

获取模块，用于获取应用程序内媒体文件的属性列表的操作权限;

读写模块，用于读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内;

保存模块，用于将所述媒体文件重新保存。

进一步的，所述装置还包括:

逻辑处理模块，用于对应用程序内产生的用户信息进行逻辑处理。

与现有技术相比，本申请实施例提供的一种基于应用程序的用户信息的隐藏方法及装置，通过将应用程序内产生的用户信息写入应用程序的媒体文件的属性列表内，如此用户信息得到隐藏，在移动终端本地文件夹内不易被找到和获取，从而达到防止产生应用程序内的用户信息被泄露目的。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中:

图 1 为本申请实施例一提供的基于应用程序的用户信息的隐藏方法的流程示意图;

图 2 为本申请实施例二提供的基于应用程序的用户信息的隐藏方法的流程示意图;

图 3 为本申请实施例三提供的基于应用程序的用户信息的隐藏装置的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

图 1 为本申请实施例提供的基于应用程序的用户信息的隐藏方法的流程示意图。下面将结合图 1 对本申请实施例提供的基于应用程序的用户信息的隐藏的方法进行详细介绍，如图 1 所示，本申请实施例提供的基于应用程序的用户信息的隐藏的方法包括以下步骤。

步骤 S101: 获取应用程序内媒体文件的属性列表的操作权限。

在本申请实施例中，移动终端应用程序在运行过程中，会产生与用户操作对应的用户信息，该用户信息包括涉及用户敏感、机密的信息，上述用户信息自动保存至移动终端本地。上述应用程序可以为各类安装于移动终端的应用程序，如支付类、交友类应用程序。以支付类应用程序为例，用户在使用、操作支付类应用程序的过程中，会产生登录账号、登录密码、身份证号、手机号、银行卡号及支付密码等敏感、机密的用户信息。上述用户信息中，如登陆密码、支付密码为机密的用户信息，登陆账号、身份证、手机号、银行卡号为敏感信息。

进一步的，应用程序在运行过程中，不同的业务类型或应用场景对应不同的用户信息。继续以支付类应用程序为例，在支付的应用场景下，会产生包括与支付相关的敏感、机密的用户信息。另外，在好友聊天的应用场景下，又会产生涉及聊天信息的用户信息。

在本步骤中，应用程序内的媒体文件可以位于应用程序的安装目录下，可以作为用于保存上述用户信息的载体。不同类型的用户信息可以保存于不同的媒体文件内。进一步的，上述用户信息可以保存于媒体文件的属性列表内，属性列表内包括用于描述媒体文件信息的属性信息。上述媒体文件可以为图片、音频及视频文件中的任意一种。优选地，上述媒体文件可以为图片文件。上述媒体文件可以作为用于应用程序图面显示的一部分预先打包至应用程序安装包内，当应用程序安装后，上述媒体文件就位于应用程序的安装目录下。

用户可以通过鼠标针移动到媒体文件，按鼠标右键，将鼠标通过点击媒体文件属性选项，再点击详细信息就可以看到关于媒体文件的一个属性列表，其内包括属性标识及对应的属性值。比如，在照片的属性列表内，包括名称、项目类型、创建日期、修改日期等在内的属性标识及属性标识对应的属性值。

进一步的，获取应用程序内媒体文件的属性列表的操作权限，具体包括:

获取应用程序内媒体文件的句柄；通过所述媒体文件的句柄，来获取应用程序内媒体文件的属性列表的读取、写入权限。

媒体文件的句柄（file handle）也可以称为媒体文件的对象指针。句柄是指使用的一个唯一的整数值，即一个 4 字节(64 位程序中为 8 字节)长的数值，来标识应用程序中的不同对象和同类中的不同的实例。通过获取到的媒体文件的句柄，应用程序可使用这对句柄对媒体文件，即媒体文件的

属性列表进行读取、写入信息的操作。

步骤 S102: 读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内。

在本实施例中，由于获取了媒体文件的句柄，因此媒体文件的属性列表可以作为一个可进行读写操作的对象。媒体文件的属性列表内包括用于描述媒体文件的属性信息。

上述媒体文件的属性列表被读取至移动终端的内存中，并在移动终端的内存中将上述用户信息写入媒体文件的属性列表内。

上述将应用程序内产生的用户信息写入所述媒体文件的属性列表内，具体包括:

将应用程序内产生的用户信息以键值对的形式写入所述媒体文件的属性列表内。

在应用程序运行过程中会产生了与用户操作相关的用户信息，如敏感信息、机密信息等。该用户信息可以是未经加密的明文，该用户信息可以直接写入媒体文件的属性列表内。

比如，在应用程序运行过程中，产生了账户密码，其保存于本地。为了避免用户的账户密码被盗取，该账户密码可以以键值对（Key-Value）的形式写入媒体文件的属性列表内，以便隐藏该账户密码信息。具体的，账户密码对应的属性标识 Key 可以被命名为 Password，账户密码的属性值 Value 可以为一串代表密码的文字，该串文字可以为明文。当然，为了更好地隐藏及伪装账户密码，账户密码对应的属性标识 Key 可以设置为系统类的属性标识 Key，如此更不易被识别。

另外，需要说明的是，应用程序内产生的与用户操作相关的用户信息也可以为是已经加密的密文。针对用户信息的加密方法包括: MD5，DES，

RSA，SM2，SM3 等加密算法。

进一步的，不同应用场景下的产生的用户信息可以写入不同的媒体文件内。比如，在应用程序支付场景产生的用户信息（如支付密码、订单信息等）可以写入一个媒体文件中，如图片 a 中；在聊天应用场景下产生的用户信息（如聊天信息内的电话号码、银行卡号等）可以写入另一个媒体文件中，如图片 b 中。

步骤 S103：将所述媒体文件重新保存。

在本实施例中，当需要进行隐藏的用户信息均写入媒体文件的属性列表内后，将上述媒体文件重新保存。当用户后续通过鼠标针移动到该媒体文件，按鼠标右键，将鼠标通过点击媒体文件属性选项，再点击详细信息就可以看到写入属性列表内的用户信息已存于所述媒体文件的属性列表内了。

具体地，若媒体文件保存成功，则该媒体文件保存于应用程序的安装路径下，此时用户信息伪装成功。

若媒体文件保存失败，则可每隔一个预设时间段（如 3 至 5 秒）自动重新保存，预设重新保存的次数可以是 3 次。若在 3 次重新保存的机会内媒体文件保存成功，则表示用户信息的伪装成功。若重新保存超过 3 次后，媒体文件仍未保存成功，则将这次保存失败保存至失败队列中。

当应用程序内再次产生涉及敏感、机密信息的用户信息时，用户信息写入媒体文件并且媒体文件成功保存后，自动调用失败队列，重新保存媒体文件直到其成功保存，如果还是保存失败，则将这次任务重新加入新的失败队列，重复上述过程直到媒体文件保存成功为止。

图 2 为本申请实施二例提供的基于应用程序的用户信息的隐藏的方法流程示意图。下面将结合图 2 对本申请实施例二提供的基于应用程序的用

户信息的隐藏的方法进行详细介绍，如图 2 所示，本申请实施例二提供的基于应用程序的用户信息的隐藏的方法包括以下步骤。

步骤 S201：获取应用程序内媒体文件的属性列表的操作权限。

在本实施例中，此步骤与本申请实施例一提供的基于应用程序的用户信息的隐藏方法的步骤 S101 基本相同，此处不再赘述。

步骤 S202：对应用程序内产生的用户信息进行逻辑处理。

在本实施例中，为了防止产生于应用程序内的用户信息（如敏感、机密的用户信息）轻易泄露，需要对应用程序内的上述用户信息预先进行逻辑处理。需要说明的是，上述逻辑处理为可逆的逻辑处理，即针对用户信息的逻辑处理过程可逆。

对应用程序内产生的用户信息进行逻辑处理，具体包括：

通过对称加密算法，对应用程序内产生的用户信息进行对称加密处理。

当然，需要说明的是，该用户信息在逻辑处理前也可以通过 MD5，DES，RSA，SM2，SM3 等加密算法进行一次加密处理。

步骤 S203：读取应用程序内媒体文件的属性列表并将应用程序内经过逻辑处理的用户信息写入所述媒体文件的属性列表内。

需要说明的是，在本实施例中，经过逻辑处理后的用户信息也可以以键值对（Key-Value）的形式写入媒体文件的属性列表内，以便隐藏该用户信息。以用户信息为账户密码为例，账户密码对应的属性标识 Key 可以被命名为 Password，账户密码的属性值 Value 可以为一串逻辑处理后的文字或字符串。

步骤 S204：将所述媒体文件重新保存。

在本实施例中，当需要进行隐藏的用户信息均写入媒体文件的属性列表内后，将上述媒体文件重新保存。此步骤与本申请实施例一提供的基于应用程序的用户信息的隐藏方法的步骤S103基本相同，此处不再赘述。

以上为本申请实施例提供的基于应用程序的用户信息的隐藏方法，基于同样的思路，本申请实施例三还提供了基于应用程序的用户信息的隐藏装置。参见图 3，该图示出了本申请实施例三提供的基于应用程序的用户信息的隐藏装置的结构，其具体包括:

获取模块 301，用于获取应用程序内媒体文件的属性列表的操作权限;

逻辑处理模块 302，用于对应用程序内产生的用户信息进行逻辑处理;

读写模块 303，用于读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息或经过逻辑处里的用户信息写入媒体文件的属性列表内;

保存模块 304，用于将媒体文件重新保存。

需要说明的是，上述用属性列表内包括描述媒体文件的属性信息。户信息为敏感、机密的信息，上述媒体文件包括照片、音频及视频文件。另外，上述用户信息也可以为预先加密过的用户信息。

针对应用程序内产生的用户信息进行逻辑处理为可逆的逻辑处理，比如，该逻辑处理可以为对称加密。

综上所述，本申请实施例提供的一种基于应用程序的用户信息的隐藏方法及装置，通过将应用程序内产生的用户信息写入应用程序的媒体文件的属性列表内，如此用户信息得到隐藏，在移动终端本地文件夹内不易被找到和获取，从而达到防止产生应用程序内的用户信息被泄露目的。

在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上

的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片 2。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用 “逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language ） 与 Verilog2。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入

微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。

为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一

个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介

质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

还需要说明的是，术语“包括”、“包含”或者其任何其他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、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种基于应用程序的用户信息的隐藏方法，其特征在于，其包括:

获取应用程序内媒体文件的属性列表的操作权限;

读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内;

将所述媒体文件重新保存。

2、如权利要求 1 所述的方法，其特征在于，所述用户信息包括敏感或机密的信息。

3、如权利要求 1 所述的方法，其特征在于，所述获取应用程序内媒体文件的属性列表的操作权限，具体包括:

获取应用程序内媒体文件的句柄;

通过媒体文件的句柄，来获取应用程序内媒体文件的属性列表的读取、写入权限。

4、如权利要求 1 所述的方法，其特征在于，所述将应用程序内产生的用户信息写入所述媒体文件的属性列表内，具体包括:

将应用程序内产生的用户信息以键值对的形式写入所述媒体文件的属性列表内。

5、如权利要求 1 所述的方法，其特征在于，所述媒体文件包括照片、音频及视频文件。

6、如权利要求 1 所述的方法，其特征在于，所述用户信息为加密过

的用户信息。

7、一种基于应用程序的用户信息的隐藏方法，其特征在于，其包括:

获取应用程序内媒体文件的属性列表的操作权限;

对应用程序内产生的用户信息进行逻辑处理;

读取应用程序内媒体文件的属性列表并将应用程序内经过逻辑处理的用户信息写入所述媒体文件的属性列表内;

将所述媒体文件重新保存。

8、如权利要求 7 所述的方法，其特征在于，所述用户信息包括敏感或机密的信息。

9、如权利要求 7 所述的方法，其特征在于，所述获取应用程序内媒体文件的属性列表的操作权限，具体包括:

获取应用程序内媒体文件的句柄;

通过媒体文件的句柄，来获取应用程序内媒体文件的属性列表的读取、写入权限。

10、如权利要求 7 所述的方法，其特征在于，所述将应用程序内产生的用户信息写入所述媒体文件的属性列表内，具体包括:

将应用程序内产生的用户信息以键值对的形式写入所述媒体文件的属性列表内。

11、如权利要求 7 所述的方法，其特征在于，所述媒体文件包括照片、音频及视频文件。

12、如权利要求 7 所述的方法，其特征在于，所述用户信息为加密过的用户信息。

13、如权利要求 7 所述的方法，其特征在于，所述对应用程序内产生的用户信息进行逻辑处理，具体包括:

对应用程序内产生的用户信息进行可逆的逻辑处理。

14、如权利要求 7 所述的方法，其特征在于，所述对应用程序内产生的用户信息进行逻辑处理，具体包括:

通过对称加密算法，对应用程序内产生的用户信息进行对称加密处理。

15、一种基于应用程序的用户信息的隐藏装置，其特征在于，其包括:

获取模块，用于获取应用程序内媒体文件的属性列表的操作权限;

读写模块，用于读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内;

保存模块，用于将所述媒体文件重新保存。

16、如权利要求 15 所述的装置，其特征在于，所述装置还包括:

逻辑处理模块，用于对应用程序内产生的用户信息进行逻辑处理。

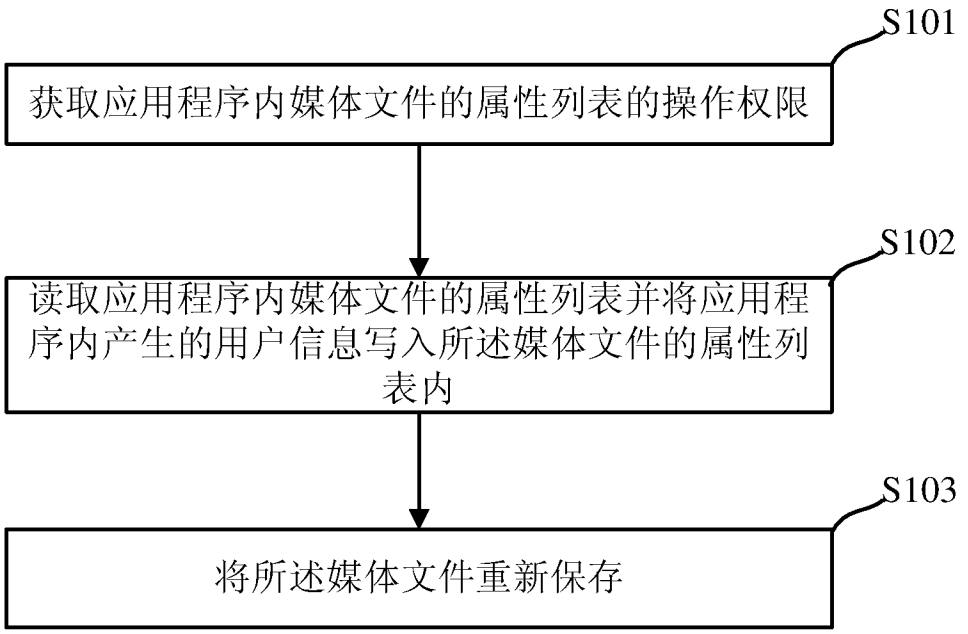
S101
获取应用程序内媒体文件的属性列表的操作权限
S102
读取应用程序内媒体文件的属性列表并将应用程序内产生的用户信息写入所述媒体文件的属性列表内
S103
将所述媒体文件重新保存

图 1

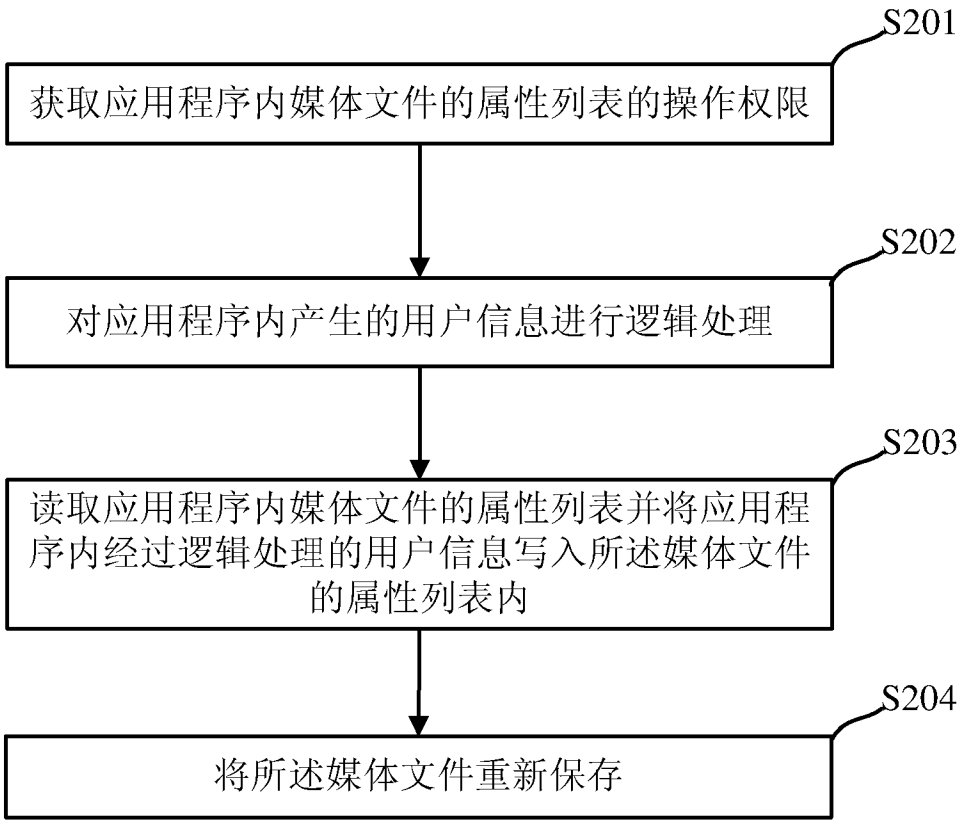
S201
获取应用程序内媒体文件的属性列表的操作权限
S202
对应用程序内产生的用户信息进行逻辑处理
S203
读取应用程序内媒体文件的属性列表并将应用程序内经过逻辑处理的用户信息写入所述媒体文件的属性列表内
S204
将所述媒体文件重新保存

图 2

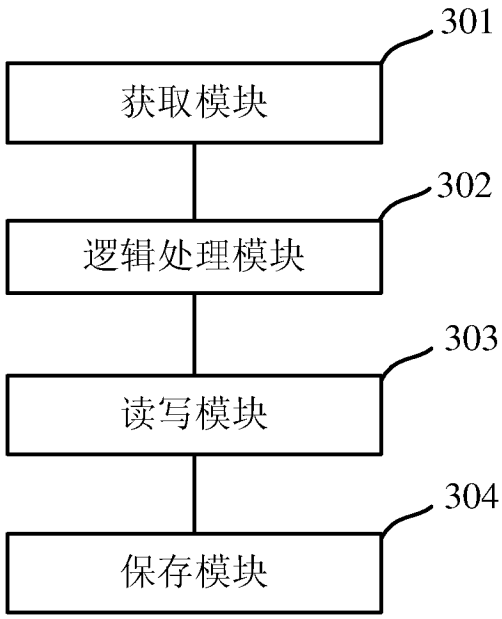

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077279

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 (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)

CNTXT, CNABS, TWTXT, CNKI, DWPI: media, secret, privacy, store, attribute, property, list, information, file, document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101114256 A (ARACHNOID BIOMETRICS IDENTIFICATION TECHNOLOGIES CO., LTD.) 30 January 2008 (30.01.2008) claims 11-17, and description, page 1	1-16
A	CN 104200171 A (INSTITUTE OF ADVANCED TECHNOLOGY, UNIVERSITY SCIENCE AND TECHNOLOGY OF CHINA) 10 December 2014 (10.12.2014) the whole document	1-16

☐ 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
16 June 2017	30 June 2017

Name and mailing address of the ISA
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, Fudong
Telephone No. (86-10) 62411855

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/077279

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101114256 A	30 January 2008	CN 101114256 B	12 May 2010
CN 104200171 A	10 December 2014	None	

国际检索报告

国际申请号
PCT/CN2017/077279

A. 主题的分类

G06F 21/62(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））

CNTXT;CNABS;TWTXT;CNKI,DWPI:媒体，密，储，属性，列表，信息，文件，media，secret, privacy, store, attribute, property, list, information, file, 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
X	CN 101114256 A (知网生物识别科技股份有限公司) 2008年 1月 30日 (2008-01-30) 权利要求11-17、说明书第1页	1-16
A	CN 104200171 A (中国科学技术大学先进技术研究院) 2014年 12月 10日 (2014-12-10) 全文	1-16

☐ 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
2017年 6月 16日	2017年 6月 30日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 王阜东 电话号码 (86-10)62411855

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/077279

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 101114256 A	2008年 1月 30日	CN 101114256 B	2010年 5月 12日
CN 104200171 A	2014年 12月 10日	无	