

(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
2016 年 6 月 23 日 (23.06.2016)



(10) 国际公布号
WO 2016/095623 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04N 7/18 (2006.01)
- (21) 国际申请号: PCT/CN2015/093860
- (22) 国际申请日: 2015 年 11 月 5 日 (05.11.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410804324.0 2014 年 12 月 19 日 (19.12.2014) CN
- (71) 申请人: 小米科技有限责任公司 (XIAOMI INC.) [CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层, Beijing 100085 (CN)。
- (72) 发明人: 王巍 (WANG, Wei); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。张波 (ZHANG, Bo); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。高自光 (GAO, Ziguang); 中国北京市海淀区清河中街 68 号

华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。殷明君 (YIN, Mingjun); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。

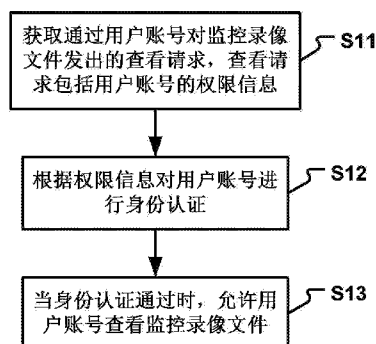
(74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路 5 号远大中心 B 座 1802, 1803, 1805, Beijing 100101 (CN)。

(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, 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。

[见续页]

(54) Title: METHOD AND APPARATUS FOR PROCESSING SURVEILLANCE VIDEO

(54) 发明名称: 监控录像处理方法及装置



S11 Acquiring a viewing request sent out for a surveillance video file via a user account, the viewing request comprising authority information of the user account
S12 Performing identity authentication on the user account according to the authority information
S13 When the identity authentication is passed, allowing the user account to check the surveillance video file

图1/fig. 1

(57) Abstract: The present invention relates to a method and apparatus for processing a surveillance video. The method comprises: acquiring a viewing request sent out for a surveillance video file via a user account, the viewing request comprising authority information of the user account; performing identity authentication on the user account according to the authority information; and when the identity authentication is passed, allowing the user account to view the surveillance video file. The present invention is used for prohibiting optional checking for surveillance video files.

(57) 摘要: 本公开是关于一种监控录像处理方法及装置。所述方法包括: 获取通过用户账号对所述监控录像文件发出的查看请求, 所述查看请求包括所述用户账号的权限信息; 根据所述权限信息对所述用户账号进行身份认证; 当身份认证通过时, 允许所述用户账号查看所述监控录像文件。本公开用于禁止对监控录像文件的随意查看。



WO 2016/095623 A1



(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)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

监控录像处理方法及装置

5 本申请基于申请号为 201410804324.0、申请日为 2014-12-19 的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开涉及计算机技术领域，尤其涉及一种监控录像处理方法及装置。

10 背景技术

随着传统摄像机与网络技术的结合，网络摄像头可以将影像透过网络传至地球另一端，且远端的浏览者通过标准的网络浏览器（如"Microsoft IE 或 Netscape)即可监视其影像。

15 相关技术中，网络摄像头除了可以将监控录像保存到本地以外，还可以自动传输到网络路由器上，方便用户查看监控和备份。这个功能虽然实用，但是也带来了相应的隐私问题，任何一个用户可以随意查看路由器上的监控视频。

发明内容

本公开实施例提供一种监控录像处理方法及装置。

20 根据本公开实施例的第一方面，提供一种监控录像处理方法，所述方法包括：

获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户账号的权限信息；

根据所述权限信息对所述用户账号进行身份认证；

当身份认证通过时，允许所述用户账号查看所述监控录像文件。

25 本实施例中，通过对访问监控录像文件的用户进行身份认证，仅允许通过身份认证的用户查看监控录像，使得监控录像无法被随意查看，防止用户隐私信息泄露，有效地保护用户隐私。

可选的，所述方法还包括：

对摄像装置上传的所述监控录像文件执行隐私保护操作。

30 在可选方案中，通过对监控录像文件进行隐私保护操作，使得监控录像无法被随意查看，防止用户隐私信息泄露，有效地保护用户隐私。

可选的，所述对摄像装置上传的所述监控录像文件执行隐私保护操作，包括下列至少一个操作：

将所述监控录像文件的属性设置为隐藏；

35 对所述监控录像文件进行加密。

在可选方案中,可以通过两种方式:将监控录像文件隐藏或对监控录像文件进行加密,或这两种方式的结合,对监控录像文件进行保护,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

可选的,所述对监控录像文件进行加密,包括:

- 5 获取用于加密所述监控录像文件的文件密钥;
 根据所述文件密钥对所述监控录像文件进行加密。

在可选方案中,终端对监控录像文件进行加密,可以实现对监控录像文件进行保护,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

可选的,所述方法还包括:

- 10 将所述文件密钥分发给预设用户账号。

在可选方案中,摄像装置所有者可预先设定的有访问监控录像文件权限的用户账号,终端将文件密钥分发给这样用户,使得这些用户可以查看监控录像文件。这样,使得只有具有访问权限的用户才能查看终端上的监控录像文件,有效地保护保护用户隐私。

可选的,所述方法还包括:

- 15 获取所述预设用户账号的用户私钥;
 根据所述文件密钥和所述预设用户账号的用户私钥生成所述预设用户账号的用户公钥;

将所述用户公钥发送到对应的预设用户账号,由所述预设用户账号根据所述用户公钥和所述用户私钥生成所述监控录像文件的文件密钥。

- 20 在可选方案中,基于 RSA 公开密钥密码体制,可以避免公开文件的加密密钥;同时,虽然文件的加密密钥是一定的,但各个预设用户账号的私钥可以不同,终端为各个用户账号生成的公钥也就不相同,这样即便各个用户账号的公钥被公开,其他人也不能得到文件的加密密钥,进一步提高了文件加密密钥的安全性,也提高了监控录像文件的安全性,更加有效地保护保护用户隐私。

- 25 可选的,当所述监控录像文件的属性设置为隐藏时,所述当身份认证通过时,允许所述用户账号查看所述监控录像文件,包括:

当身份认证通过时,将所述监控录像文件的属性修改为可见;
对可见的监控录像文件进行展示。

- 30 在可选方案中,当用户通过身份认证时,终端将隐藏的监控录像文件的属性修改为可见,使得通过身份认证的用户可以访问到该监控录像文件,以实现监控录像文件进行保护,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

可选的,当所述监控录像文件被加密时,所述当身份认证通过时,允许所述用户账号查看所述监控录像文件,包括:

- 35 当身份认证通过时,获取所述用户账号输入的文件密钥;
 根据所述文件密钥对所述监控录像文件进行解密;

对解密后的监控录像文件进行展示。

在可选方案中，当用户通过身份认证时，终端提示用户输入文件密钥，以便对监控录像文件进行解密并展示给用户，以实现监控录像文件进行保护，使得监控录像无法被随意查看，防止用户隐私信息泄露，有效地保护用户隐私。

- 5 可选的，所述文件密钥为拍摄所述监控录像文件的摄像装置所有者账户的用户密码，所述权限信息包括所述用户账号的用户名和用户密码；

所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

- 10 当根据所述权限信息确定所述用户账号为拍摄所述监控录像文件的摄像装置所有者账户时，使用拍摄所述监控录像文件的摄像装置所有者账户的用户密码对所述监控录像文件进行解密；

对解密后的监控录像文件进行展示。

在可选方案中，当摄像装置所有者采用自身账户的用户密码对监控录像文件进行加密时，在身份验证时确定访问者为摄像装置所有者自己时，直接为用户解密监控录像文件，以便摄像装置所有者可以方便、快速地访问监控录像文件。

- 15 根据本公开实施例的第二方面，提供一种监控录像处理装置，包括：

第一获取模块，用于获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户账号的权限信息

认证模块，用于根据所述权限信息对所述用户账号进行身份认证；

查看模块，用于当身份认证通过时，允许所述用户账号查看所述监控录像文件。

- 20 可选的，所述装置还包括：

执行模块，用于对所述摄像装置上传的所述监控录像文件执行隐私保护操作。

可选的，所述执行模块包括下列至少一个子模块：

设置子模块，用于将所述监控录像文件的属性设置为隐藏；

加密子模块，用于对所述监控录像文件进行加密。

- 25 可选的，所述加密子模块，用于获取用于加密所述监控录像文件的文件密钥；根据所述文件密钥对所述监控录像文件进行加密。

可选的，所述装置还包括：

分发模块，用于将所述文件密钥分发给预设用户账号。

可选的，所述装置还包括：

- 30 第二获取模块，用于获取所述预设用户账号的用户私钥；

生成模块，用于根据所述文件密钥和所述预设用户账号的用户私钥生成所述预设用户账号的用户公钥；

发送模块，用于将所述用户公钥发送到对应的预设用户账号，由所述预设用户账号根据所述用户公钥和所述用户私钥生成所述监控录像文件的文件密钥。

- 35 可选的，所述查看模块包括：

修改子模块，用于当所述监控录像文件的属性设置为隐藏，且身份认证通过时，将所述监控录像文件的属性修改为可见；

展示子模块，用于对可见的监控录像文件进行展示。

可选的，所述查看模块包括：

- 5 获取子模块，用于当所述监控录像文件被加密，且身份认证通过时，获取所述用户账号输入的文件密钥；

解密子模块，用于根据所述文件密钥对所述监控录像文件进行解密；

展示子模块，用于对解密后的监控录像文件进行展示。

- 10 可选的，所述文件密钥为拍摄所述监控录像文件的摄像装置所有者账户的用户密码，所述权限信息包括所述用户账号的用户名和用户密码；

所述查看模块包括：

解密子模块，用于当根据所述权限信息确定所述用户账号为拍摄所述监控录像文件的摄像装置所有者账户时，使用拍摄所述监控录像文件的摄像装置所有者账户的用户密码对所述监控录像文件进行解密；

- 15 展示子模块，用于对解密后的监控录像文件进行展示。

根据本公开实施例的第三方面，提供一种监控录像处理装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

- 20 获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户账号的权限信息；

根据所述权限信息对所述用户账号进行身份认证；

当身份认证通过时，允许所述用户账号查看所述监控录像文件。

- 25 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

- 30 图 1 是根据一示例性实施例示出的一种监控录像处理方法的流程图；
图 2 是根据另一示例性实施例示出的一种监控录像处理方法的流程图；
图 3 是根据另一示例性实施例示出的一种监控录像处理方法的流程图；
图 4 是根据另一示例性实施例示出的一种监控录像处理方法的流程图；
图 5 是根据另一示例性实施例示出的一种监控录像处理方法的流程图；
35 图 6 是根据另一示例性实施例示出的一种监控录像处理方法的流程图；

图 7 是根据另一示例性实施例示出的一种监控录像处理方法的流程图;

图 8 是根据一示例性实施例示出的一种监控录像处理装置的框图;

图 9 是根据另一示例性实施例示出的一种监控录像处理装置的框图;

图 10 是根据一示例性实施例示出的执行模块的框图;

5 图 11 是根据另一示例性实施例示出的一种监控录像处理装置的框图;

图 12 是根据另一示例性实施例示出的一种监控录像处理装置的框图;

图 13 是根据一示例性实施例示出的查看模块的框图;

图 14 是根据另一示例性实施例示出的查看模块的框图;

图 15 是根据另一示例性实施例示出的查看模块的框图;

10 图 16 是根据一示例性实施例示出的一种用于监控录像处理的装置的框图;

图 17 是根据一示例性实施例示出的一种用于监控录像处理的装置的框图。

具体实施方式

这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图
15 时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

摄像装置(如监控摄像头)拍摄到的监控录像文件上传到终端设备(计算机或路由器),本公开主要对终端设备上的监控录像文件进行隐私保护。

20 图 1 是根据一示例性实施例示出的一种监控录像处理方法的流程图,如图 1 所示,摄像装置将监控录像文件上传到终端,该监控录像处理方法用于终端中,包括以下步骤。

在步骤 S11 中,获取通过用户账号对监控录像文件发出的查看请求,查看请求包括用户账号的权限信息;

在步骤 S12 中,根据权限信息对用户账号进行身份认证;

25 在步骤 S13 中,当身份认证通过时,允许用户账号查看监控录像文件。

本实施例中,通过对访问监控录像文件的用户进行身份认证,仅允许通过身份认证的用户查看监控录像,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

30 图 2 是根据另一示例性实施例示出的一种监控录像处理方法的流程图,如图 2 所示,可选的,该方法还包括:

在步骤 S10 中,对摄像装置上传的监控录像文件执行隐私保护操作。

在可选方案中,通过对监控录像文件进行隐私保护操作,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

可选的,步骤 S10 包括下列至少一个操作

35 将监控录像文件的属性设置为隐藏;

对监控录像文件进行加密。

在可选方案中,可以通过两种方式:将监控录像文件隐藏或对监控录像文件进行加密,或这两种方式的结合,对监控录像文件进行保护,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

5 图 3 是根据另一示例性实施例示出的一种监控录像处理方法的流程图,如图 3 所示,可选的,对监控录像文件进行加密,包括:

在步骤 S31 中,获取用于加密监控录像文件的文件密钥;

在步骤 S32 中,根据文件密钥对监控录像文件进行加密。

10 在可选方案中,终端对监控录像文件进行加密,加密用的文件密钥可以是摄像装置所有者预先设定的,如摄像装置所有者在终端上的用户密码;加密用的文件密钥可以是终端生成的,无论摄像装置所有者还是其他用户都无法获知实际加密监控录像文件的文件密钥,进一步保证终端上存储的监控录像文件的安全性。这些加密方法,都可以实现对监控录像文件进行保护,使得监控录像无法被随意查看,防止用户隐私信息泄露,有效地保护用户隐私。

15 可选的,该方法还包括:

将文件密钥分发给预设用户账号。

在可选方案中,摄像装置所有者可预先设定的有访问监控录像文件权限的用户账号,终端将文件密钥分发给这样用户,使得这些用户可以查看监控录像文件。这样,使得只有具有访问权限的用户才能查看终端上的监控录像文件,有效地保护保护用户隐私。

20 图 4 是根据另一示例性实施例示出的一种监控录像处理方法的流程图,如图 4 所示,可选的,该方法还包括:

在步骤 S41 中,获取预设用户账号的用户私钥;

在步骤 S42 中,根据文件密钥和预设用户账号的用户私钥生成预设用户账号的用户公钥;

25 在步骤 S43 中,将用户公钥发送到对应的预设用户账号,由预设用户账号根据用户公钥和用户私钥生成监控录像文件的文件密钥。

在可选方案中,基于 RSA 公开密钥密码体制,终端根据预设用户账号的私钥和自身加密文件所用的密钥,生成给预设用户账号的公钥,其他用户可以根据公钥和自身的私钥计算出加密文件的密钥,这样,这些用户就可以访问终端上的录像文件。通过这种加密方式,可以避免公开文件的加密密钥;同时,虽然文件的加密密钥是一定的,但各个预设用户账号的私钥可以不同,终端为各个用户账号生成的公钥也就不相同,这样即便各个用户账号的公钥被公开,其他人也不能得到文件的加密密钥,进一步提高了文件加密密钥的安全性,也提高了监控录像文件的安全性,更加有效地保护保护用户隐私。

30 图 5 是根据另一示例性实施例示出的一种监控录像处理方法的流程图,如图 5 所示,可选的,当监控录像文件的属性设置为隐藏时,步骤 S13 包括:

在步骤 S51 中, 当身份认证通过时, 将监控录像文件的属性修改为可见;

在步骤 S52 中, 对可见的监控录像文件进行展示。

在可选方案中, 当用户通过身份认证时, 终端将隐藏的监控录像文件的属性修改为可见, 使得通过身份认证的用户可以访问到该监控录像文件, 以实现对该监控录像文件进行保护, 使得监控录像无法被随意查看, 防止用户隐私信息泄露, 有效地保护用户隐私。

图 6 是根据另一示例性实施例示出的一种监控录像处理方法的流程图, 如图 6 所示, 可选的, 当监控录像文件被加密时, 步骤 S13 包括:

在步骤 S61 中, 当身份认证通过时, 获取用户账号输入的文件密钥;

在步骤 S62 中, 根据文件密钥对监控录像文件进行解密;

在步骤 S63 中, 对解密后的监控录像文件进行展示。

在可选方案中, 当用户通过身份认证时, 终端提示用户输入文件密钥, 以便对监控录像文件进行解密并展示给用户, 以实现对该监控录像文件进行保护, 使得监控录像无法被随意查看, 防止用户隐私信息泄露, 有效地保护用户隐私。

图 7 是根据另一示例性实施例示出的一种监控录像处理方法的流程图, 如图 7 所示, 可选的, 文件密钥为拍摄监控录像文件的摄像装置所有者账户的用户密码, 权限信息包括用户账号的用户名和用户密码; 步骤 S13 包括:

在步骤 S71 中, 当根据权限信息确定用户账号为拍摄监控录像文件的摄像装置所有者账户时, 使用拍摄监控录像文件的摄像装置所有者账户的用户密码对监控录像文件进行解密;

在步骤 S72 中, 对解密后的监控录像文件进行展示。

在可选方案中, 当摄像装置所有者采用自身账户的用户密码对监控录像文件进行加密时, 在身份验证时确定访问者为摄像装置所有者自己时, 直接为用户解密监控录像文件, 以便摄像装置所有者可以方便、快速地访问监控录像文件。

图 8 是根据一示例性实施例示出的一种监控录像处理装置的框图。如图 6 所示, 该装置包括第一获取模块 81, 认证模块 82 和查看模块 83。

第一获取模块 81 被配置为获取通过用户账号对所述监控录像文件发出的查看请求, 所述查看请求包括所述用户账号的权限信息

认证模块 82 被配置为根据所述权限信息对所述用户账号进行身份认证;

查看模块 83 被配置为当身份认证通过时, 允许所述用户账号查看所述监控录像文件。

图 9 是根据另一示例性实施例示出的一种监控录像处理装置的框图。如图 9 所示, 可选的, 该装置还包括:

执行模块 84 被配置为对所述摄像装置上传的所述监控录像文件执行隐私保护操作。

图 10 是根据一示例性实施例示出的执行模块的框图。如图 10 所示, 可选的, 执行模块 84 所述执行模块包括下列至少一个子模块:

设置子模块 101，用于将所述监控录像文件的属性设置为隐藏；

加密子模块 102，用于对所述监控录像文件进行加密。

可选的，所述加密子模块 102，用于获取用于加密所述监控录像文件的文件密钥；根据所述文件密钥对所述监控录像文件进行加密。

5 图 11 是根据另一示例性实施例示出的一种监控录像处理装置的框图。如图 11 所示，可选的，所述装置还包括：

分发模块 85，用于将所述文件密钥分发给预设用户账号。

图 12 是根据另一示例性实施例示出的一种监控录像处理装置的框图。如图 12 所示，可选的，所述装置还包括：

10 第二获取模块 86，用于获取所述预设用户账号的用户私钥；

生成模块 87，用于根据所述文件密钥和所述预设用户账号的用户私钥生成所述预设用户账号的用户公钥；

发送模块 88，用于将所述用户公钥发送到对应的预设用户账号，由所述预设用户账号根据所述用户公钥和所述用户私钥生成所述监控录像文件的文件密钥。

15 图 13 是根据一示例性实施例示出的查看模块的框图。如图 13 所示，可选的，所述查看模块 83 包括：

修改子模块 131，用于当所述监控录像文件的属性设置为隐藏，且身份认证通过时，将所述监控录像文件的属性修改为可见；

展示子模块 132，用于对可见的监控录像文件进行展示。

20 图 14 是根据另一示例性实施例示出的查看模块的框图。如图 14 所示，可选的，所述查看模块 83 包括：

获取子模块 141，用于当所述监控录像文件被加密，且身份认证通过时，获取所述用户账号输入的文件密钥；

解密子模块 142，用于根据所述文件密钥对所述监控录像文件进行解密；

25 展示子模块 143，用于对解密后的监控录像文件进行展示。

图 15 是根据另一示例性实施例示出的查看模块的框图。如图 15 所示，可选的，所述文件密钥为拍摄所述监控录像文件的摄像装置所有者账户的用户密码，所述权限信息包括所述用户账号的用户名和用户密码；所述查看模块 83 包括：

30 解密子模块 151，用于当根据所述权限信息确定所述用户账号为拍摄所述监控录像文件的摄像装置所有者账户时，使用拍摄所述监控录像文件的摄像装置所有者账户的用户密码对所述监控录像文件进行解密；

展示子模块 152，用于对解密后的监控录像文件进行展示。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

35 本公开还提供一种监控录像处理装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户

5 账号的权限信息；

根据所述权限信息对所述用户账号进行身份认证；

当身份认证通过时，允许所述用户账号查看所述监控录像文件。

10 图 16 是根据一示例性实施例示出的一种用于监控录像处理的装置的框图。例如，装置 1600 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

如图 16 所示，装置 1600 可以包括以下一个或多个组件：处理组件 1602，存储器 1604，电源组件 1606，多媒体组件 1608，音频组件 1610，输入/输出（I/O）的接口 1612，传感器组件 1614，以及通信组件 1616。

15 处理组件 1602 通常控制装置 1600 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理组件 1602 可以包括一个或多个处理器 1620 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 1602 可以包括一个或多个模块，便于处理组件 1602 和其他组件之间的交互。例如，处理组件 1602 可以包括多媒体模块，以方便多媒体组件 1608 和处理组件 1602 之间的交互。

20 存储器 1604 被配置为存储各种类型的数据以支持在设备 1600 的操作。这些数据的示例包括用于在装置 1600 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 1604 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器（SRAM），电可擦除可编程只读存储器（EEPROM），可擦除可编程只读存储器（EPROM），可编程只读存储器（PROM），只读存储器（ROM），磁存储器，快闪存储器，磁盘或光盘。

25 电源组件 1606 为装置 1600 的各种组件提供电力。电源组件 1606 可以包括电源管理系统，一个或多个电源，及其他与为装置 1600 生成、管理和分配电力相关联的组件。

30 多媒体组件 1608 包括在所述装置 1600 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器（LCD）和触摸面板（TP）。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 1608 包括一个前置摄像头和/或后置摄像头。当设备 1600 处于操作模式，如拍摄模式或视频模式时，前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

35 音频组件 1610 被配置为输出和/或输入音频信号。例如，音频组件 1610 包括一个麦

麦克风（MIC），当装置 1600 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 1604 或经由通信组件 1616 发送。在一些实施例中，音频组件 1610 还包括一个扬声器，用于输出音频信号。

5 I/O 接口 1612 为处理组件 1602 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于：主页按钮、音量按钮、启动按钮和锁定按钮。

传感器组件 1614 包括一个或多个传感器，用于为装置 1600 提供各个方面的状态评估。例如，传感器组件 1614 可以检测到设备 1600 的打开/关闭状态，组件的相对定位，例如
10 所述组件为装置 1600 的显示器和小键盘，传感器组件 1614 还可以检测装置 1600 或装置 1600 一个组件的位置改变，用户与装置 1600 接触的存在或不存在，装置 1600 方位或加速/减速和装置 1600 的温度变化。传感器组件 1614 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 1614 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 1614
15 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

通信组件 1616 被配置为便于装置 1600 和其他设备之间有线或无线方式的通信。装置 1600 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 1616 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件 1616 还包括近场通信（NFC）模块，
20 以促进短程通信。例如，在 NFC 模块可基于射频识别（RFID）技术，红外数据协会（IrDA）技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

在示例性实施例中，装置 1600 可以被一个或多个应用专用集成电路（ASIC）、数字信号处理器（DSP）、数字信号处理设备（DSPD）、可编程逻辑器件（PLD）、现场可编程门阵列（FPGA）、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。
25 上述方法。

图 17 是根据一示例性实施例示出的一种用于监控录像处理的装置的框图。例如，装置 1700 可以被提供为一路由器。参照图 17，装置 1700 包括处理组件 1722，其进一步包括一个或多个处理器，以及由存储器 1732 所代表的存储器资源，用于存储可由处理组件 1722 的执行的指令，例如应用程序。存储器 1732 中存储的应用程序可以包括一个或一个
30 以上的每一个对应于一组指令的模块。此外，处理组件 1722 被配置为执行指令，以执行上述方法。

装置 1700 还可以包括一个电源组件 1726 被配置为执行装置 1700 的电源管理，一个有线或无线网络接口 1750 被配置为将装置 1700 连接到网络，和一个输入输出（I/O）接口 1758。装置 1700 可以操作基于存储在存储器 1732 的操作系统，例如 Windows Server™，
35 Mac OS X™，Unix™，Linux™，FreeBSD™ 或类似。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器，上述指令可由装置的处理器的处理器执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器（RAM）、CD-ROM、磁带、软盘和光数据存储设备等。

- 5 一种非临时性计算机可读存储介质，当所述存储介质中的指令由终端或路由器的处理器执行时，使得终端或路由器能够执行一种监控录像处理方法，所述方法包括：

获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户账号的权限信息；

根据所述权限信息对所述用户账号进行身份认证；

- 10 当身份认证通过时，允许所述用户账号查看所述监控录像文件。

本实施例中，通过对访问监控录像文件的用户进行身份认证，仅允许通过身份认证的用户查看监控录像，使得监控录像无法被随意查看，防止用户隐私信息泄露，有效地保护用户隐私。

可选的，所述方法还包括：

- 15 对摄像装置上传的所述监控录像文件执行隐私保护操作。

在可选方案中，通过对监控录像文件进行隐私保护操作，使得监控录像无法被随意查看，防止用户隐私信息泄露，有效地保护用户隐私。

可选的，所述对摄像装置上传的所述监控录像文件执行隐私保护操作，包括下列至少一个操作：

- 20 将所述监控录像文件的属性设置为隐藏；

对所述监控录像文件进行加密。

在可选方案中，可以通过两种方式：将监控录像文件隐藏或对监控录像文件进行加密，或这两种方式的结合，对监控录像文件进行保护，使得监控录像无法被随意查看，防止用户隐私信息泄露，有效地保护用户隐私。

- 25 可选的，所述对监控录像文件进行加密，包括：

获取用于加密所述监控录像文件的文件密钥；

根据所述文件密钥对所述监控录像文件进行加密。

可选的，所述方法还包括：

将所述文件密钥分发给预设用户账号。

- 30 可选的，所述方法还包括：

获取所述预设用户账号的用户私钥；

根据所述文件密钥和所述预设用户账号的用户私钥生成所述预设用户账号的用户公钥；

- 35 将所述用户公钥发送到对应的预设用户账号，由所述预设用户账号根据所述用户公钥和所述用户私钥生成所述监控录像文件的文件密钥。

可选的，当所述监控录像文件的属性设置为隐藏时，所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

当身份认证通过时，将所述监控录像文件的属性修改为可见；

对可见的监控录像文件进行展示。

- 5 可选的，当所述监控录像文件被加密时，所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

当身份认证通过时，获取所述用户账号输入的文件密钥；

根据所述文件密钥对所述监控录像文件进行解密；

对解密后的监控录像文件进行展示。

- 10 可选的，所述文件密钥为拍摄所述监控录像文件的摄像装置所有者账户的用户密码，所述权限信息包括所述用户账号的用户名和用户密码；

所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

当根据所述权限信息确定所述用户账号为拍摄所述监控录像文件的摄像装置所有者账户时，使用拍摄所述监控录像文件的摄像装置所有者账户的用户密码对所述监控录像文件进行解密；

- 15 对解密后的监控录像文件进行展示。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

- 20

应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

权利要求

1、一种监控录像处理方法，其特征在于，包括：

获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户账号的权限信息；

5 根据所述权限信息对所述用户账号进行身份认证；

当身份认证通过时，允许所述用户账号查看所述监控录像文件。

2、根据权利要求1所述的方法，其特征在于，所述方法还包括：

对摄像装置上传的所述监控录像文件执行隐私保护操作。

3、根据权利要求2所述的方法，其特征在于，所述对摄像装置上传的所述监控录像
10 文件执行隐私保护操作，包括下列至少一个操作：

将所述监控录像文件的属性设置为隐藏；

对所述监控录像文件进行加密。

4、根据权利要求3所述的方法，其特征在于，所述对监控录像文件进行加密，包括：
获取用于加密所述监控录像文件的文件密钥；

15 根据所述文件密钥对所述监控录像文件进行加密。

5、根据权利要求4所述的方法，其特征在于，所述方法还包括：

将所述文件密钥分发给预设用户账号。

6、根据权利要求4所述的方法，其特征在于，所述方法还包括：

获取所述预设用户账号的用户私钥；

20 根据所述文件密钥和所述预设用户账号的用户私钥生成所述预设用户账号的用户公
钥；

将所述用户公钥发送到对应的预设用户账号，由所述预设用户账号根据所述用户公钥
和所述用户私钥生成所述监控录像文件的文件密钥。

7、根据权利要求3所述的方法，其特征在于，当所述监控录像文件的属性设置为隐
25 藏时，所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

当身份认证通过时，将所述监控录像文件的属性修改为可见；

对可见的监控录像文件进行展示。

8、根据权利要求5或6所述的方法，其特征在于，当所述监控录像文件被加密时，
所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

30 当身份认证通过时，获取所述用户账号输入的文件密钥；

根据所述文件密钥对所述监控录像文件进行解密；

对解密后的监控录像文件进行展示。

9、根据权利要求4所述的方法，其特征在于，所述文件密钥为拍摄所述监控录像文
35 件的摄像装置所有者账户的用户密码，所述权限信息包括所述用户账号的用户名和用户密
码；

所述当身份认证通过时，允许所述用户账号查看所述监控录像文件，包括：

当根据所述权限信息确定所述用户账号为拍摄所述监控录像文件的摄像装置所有者账户时，使用拍摄所述监控录像文件的摄像装置所有者账户的用户密码对所述监控录像文件进行解密；

5 对解密后的监控录像文件进行展示。

10、一种监控录像处理装置，其特征在于，包括：

第一获取模块，用于获取通过用户账号对所述监控录像文件发出的查看请求，所述查看请求包括所述用户账号的权限信息

认证模块，用于根据所述权限信息对所述用户账号进行身份认证；

10 查看模块，用于当身份认证通过时，允许所述用户账号查看所述监控录像文件。

11、根据权利要求 10 所述的装置，其特征在于，所述装置还包括：

执行模块，用于对所述摄像装置上传的所述监控录像文件执行隐私保护操作。

12、根据权利要求 11 所述的装置，其特征在于，所述执行模块包括下列至少一个子模块：

15 设置子模块，用于将所述监控录像文件的属性设置为隐藏；

加密子模块，用于对所述监控录像文件进行加密。

13、根据权利要求 12 所述的装置，其特征在于，所述加密子模块，用于获取用于加密所述监控录像文件的文件密钥；根据所述文件密钥对所述监控录像文件进行加密。

20 14、根据权利要求 13 所述的装置，其特征在于，所述装置还包括：

分发模块，用于将所述文件密钥分发给预设用户账号。

15、根据权利要求 13 所述的装置，其特征在于，所述装置还包括：

第二获取模块，用于获取所述预设用户账号的用户私钥；

25 生成模块，用于根据所述文件密钥和所述预设用户账号的用户私钥生成所述预设用户账号的用户公钥；

发送模块，用于将所述用户公钥发送到对应的预设用户账号，由所述预设用户账号根据所述用户公钥和所述用户私钥生成所述监控录像文件的文件密钥。

16、根据权利要求 12 所述的装置，其特征在于，所述查看模块包括：

30 修改子模块，用于当所述监控录像文件的属性设置为隐藏，且身份认证通过时，将所述监控录像文件的属性修改为可见；

展示子模块，用于对可见的监控录像文件进行展示。

17、根据权利要求 14 或 15 所述的装置，其特征在于，所述查看模块包括：

获取子模块，用于当所述监控录像文件被加密，且身份认证通过时，获取所述用户账号输入的文件密钥；

35 解密子模块，用于根据所述文件密钥对所述监控录像文件进行解密；

展示子模块,用于对解密后的监控录像文件进行展示。

18、根据权利要求 13 所述的装置,其特征在于,所述文件密钥为拍摄所述监控录像文件的摄像装置所有者账户的用户密码,所述权限信息包括所述用户账号的用户名和用户密码;

5 所述查看模块包括:

解密子模块,用于当根据所述权限信息确定所述用户账号为拍摄所述监控录像文件的摄像装置所有者账户时,使用拍摄所述监控录像文件的摄像装置所有者账户的用户密码对所述监控录像文件进行解密;

展示子模块,用于对解密后的监控录像文件进行展示。

10 19、一种监控录像处理装置,其特征在于,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器被配置为:

15 获取通过用户账号对所述监控录像文件发出的查看请求,所述查看请求包括所述用户账号的权限信息;

根据所述权限信息对所述用户账号进行身份认证;

当身份认证通过时,允许所述用户账号查看所述监控录像文件。

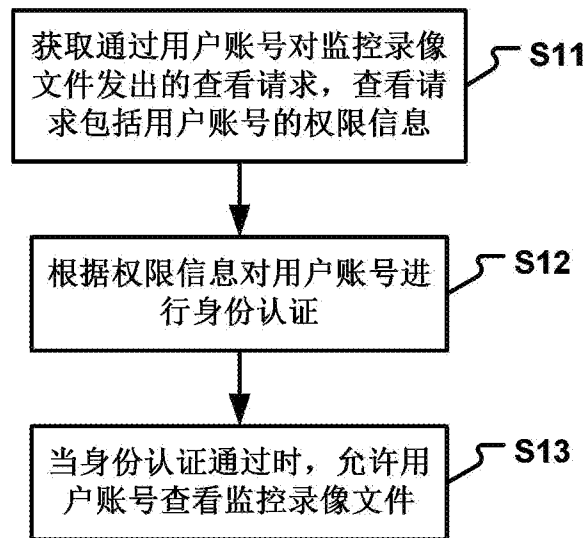


图1

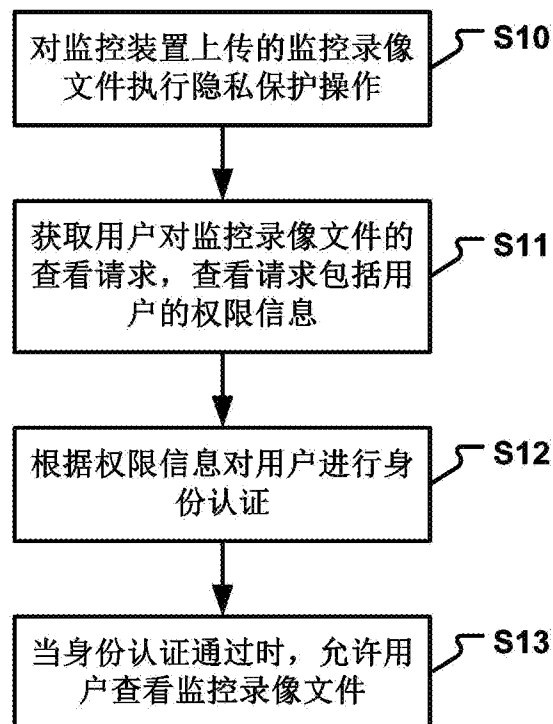


图2

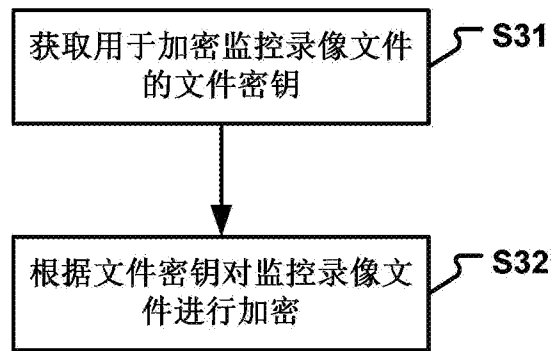


图3

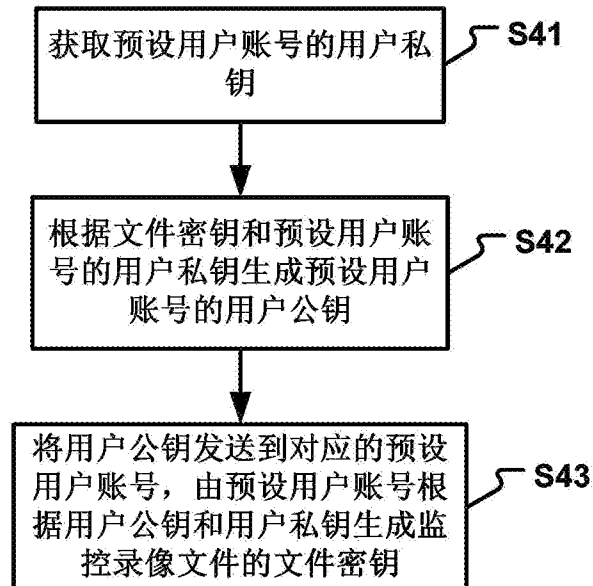


图4

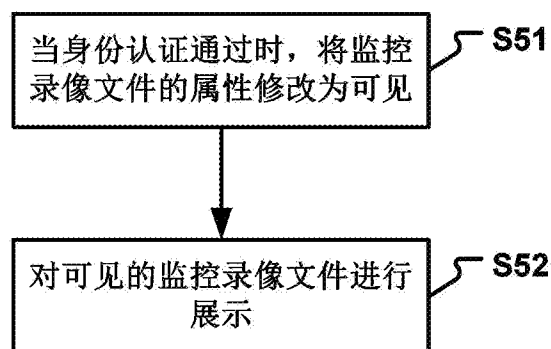


图5

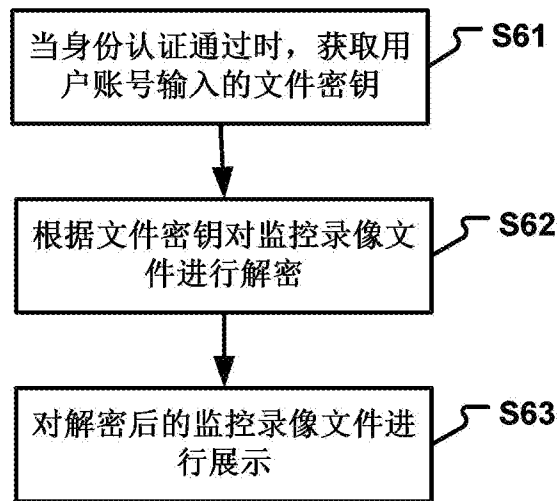


图6

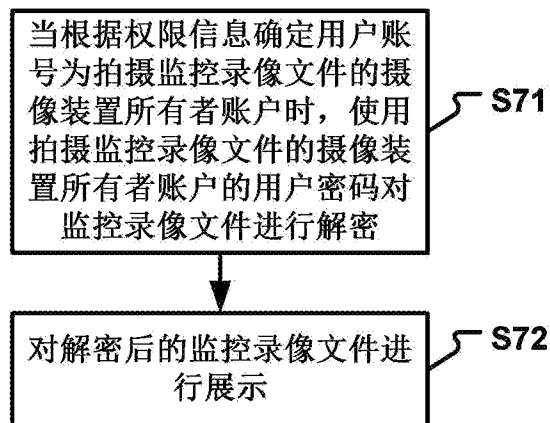


图7

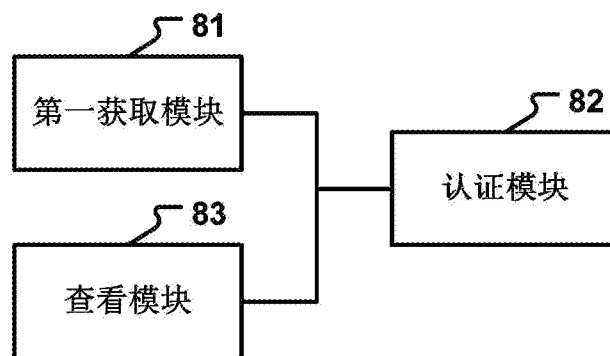


图8

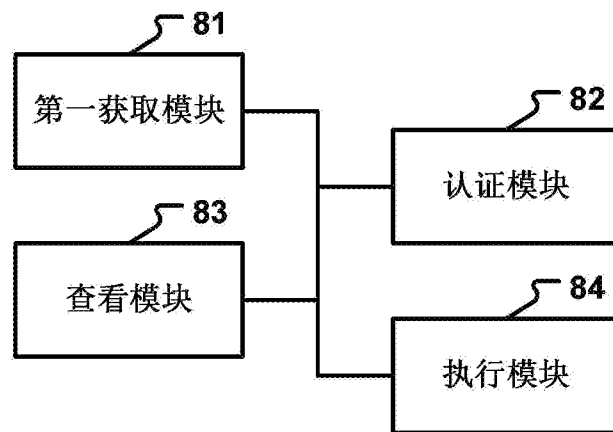


图9

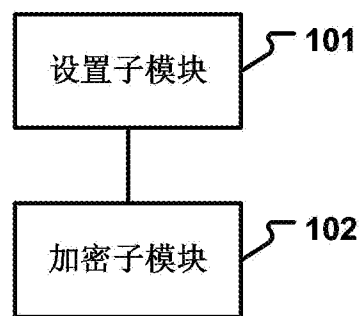


图10

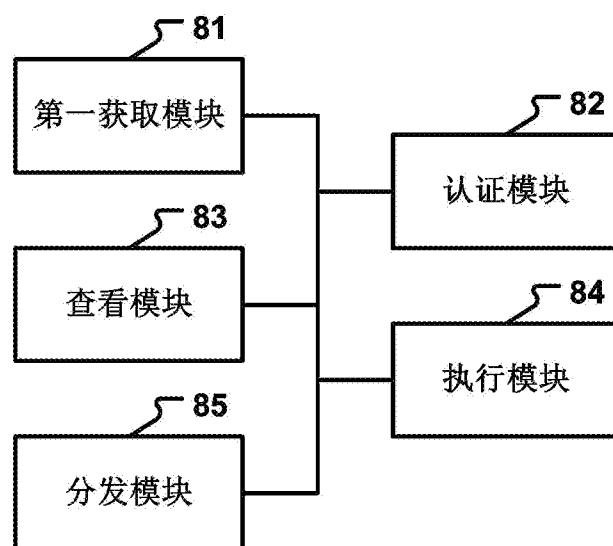


图11

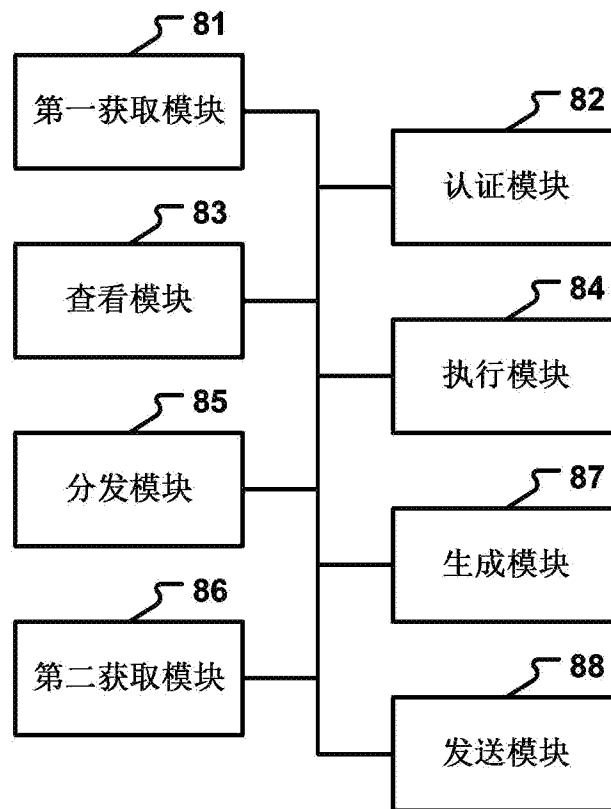


图12

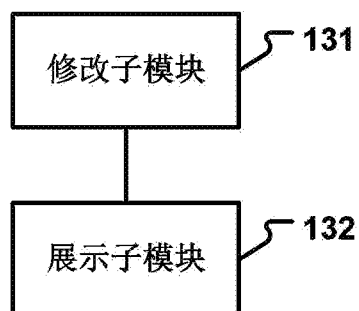


图13

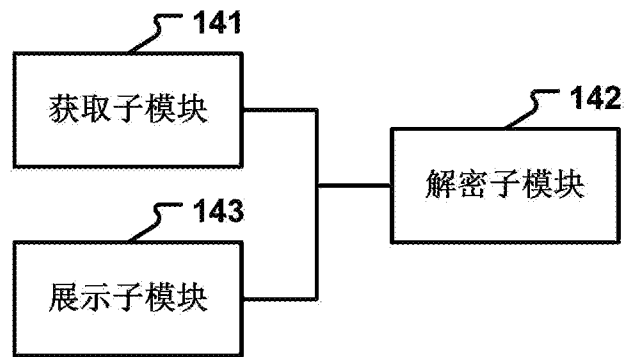


图14

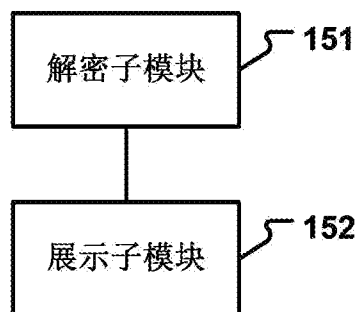


图15

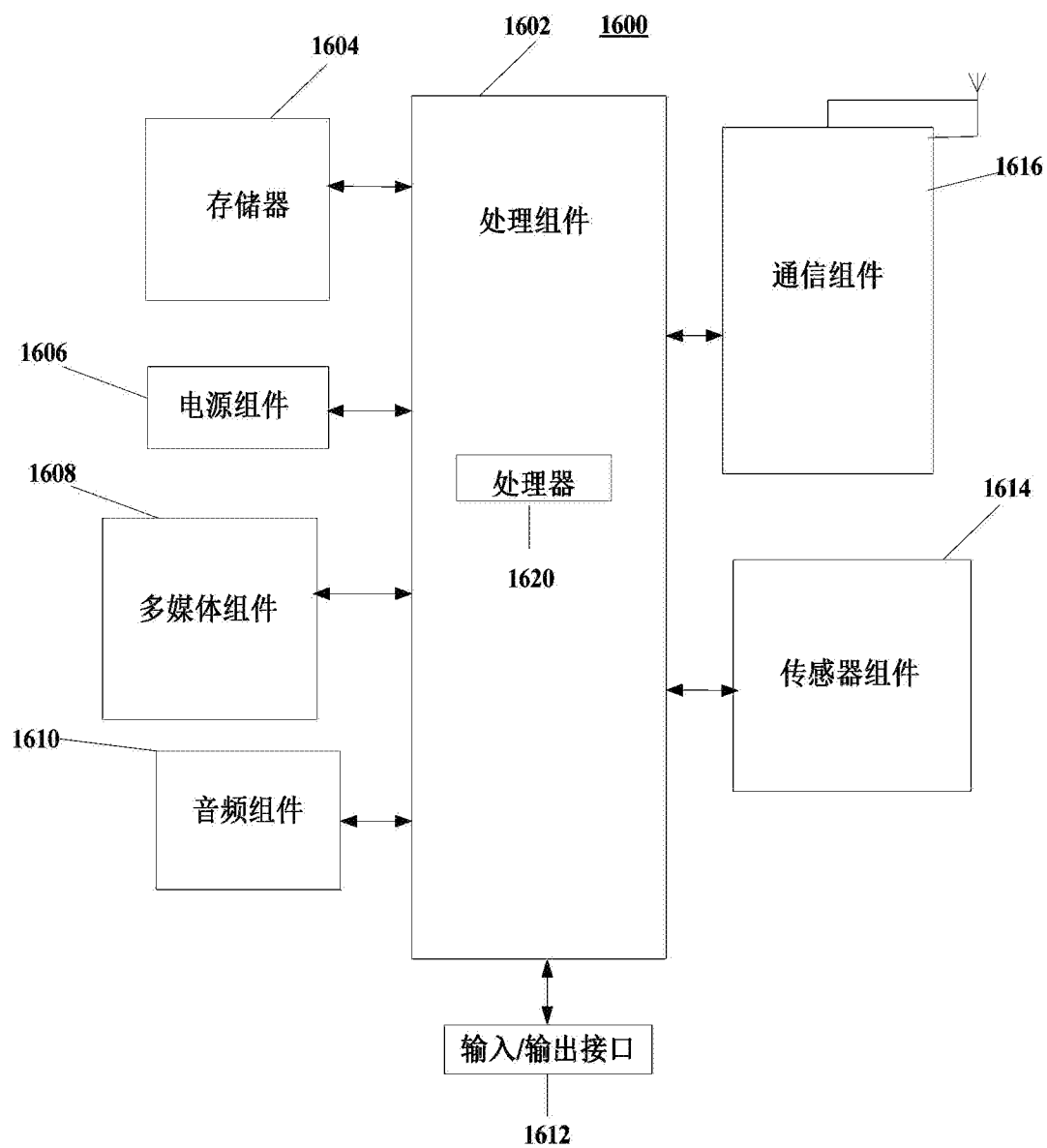


图16

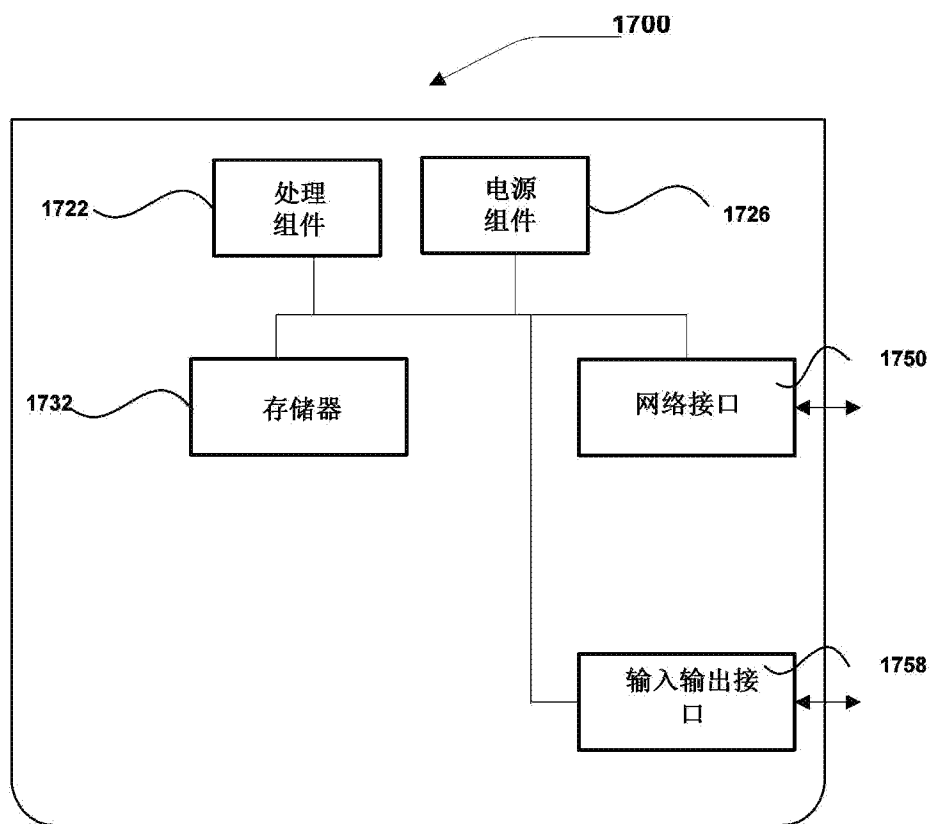


图17

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/093860

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04N 7/18 (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)

H04L, H04N

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)

CNKI, CPRSABS, CNTXT, VEN: network, camera shooting, video recording, safe, verification, surveillance, monitor, remote, camera, recorder, image, video, privacy, sensitive, authenticate, authorize, encrypt, hide

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011057787 A1 (CHUNGHWA TELECOM CO., LTD.), 10 March 2011 (10.03.2011), description, paragraphs 0035-0045 and 0050-0055, claim 2, and figures 1 and 3	1, 10, 19
Y	US 2011057787 A1 (CHUNGHWA TELECOM CO., LTD.), 10 March 2011 (10.03.2011), the same as above	2-9, 11-18
Y	CN 102055887 A (HONGFUJIN PRECISION INDUSTRY (SHENZHEN) CO., LTD. et al.), 11 May 2011 (11.05.2011), description, paragraphs 2 and 13-14, and figures 2-3	2-6, 8-9, 11-15, 17-18
Y	CN 101026822 A (JIANGSU GAOTONG SCIENCE AND TECHNOLOGY CO., LTD.), 29 August 2007 (29.08.2007), description, page 5, line 1 to page 6, line 15, and figure 4	3, 7, 12, 16
PX	CN 104486083 A (XIAOMI TECHNOLOGY CO., LTD.), 01 April 2015 (01.04.2015), claims 1-19	1-19

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search
27 January 2016 (27.01.2016)

Date of mailing of the international search report
25 February 2016 (25.02.2016)

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
CHEN, Qiong
Telephone No.: (86-10) **62411232**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/093860**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1808972 A (INTERNATIONAL BUSINESS MACHINES CORPORATION), 26 July 2006 (26.07.2006), description, page 1, paragraph 1, page 2, paragraph 2, page 3, paragraphs 2-3, page 6, paragraph 3, page 8, paragraphs 2-3 and page 14, paragraph 1 to page 15, paragraph 3, and figures 1-3	1-19
A	US 2007289012 A1 (BAIRD, L.), 13 December 2007 (13.12.2007), the whole document	1-19

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/093860

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2011057787 A1	10 March 2011	KR 101101855 B1	05 January 2012
		KR 20090023045 A	04 March 2009
		US 8026804 B2	27 September 2011
		TW 200910272 A	01 March 2009
		JP 2009059344 A	19 March 2009
		TW I338871 B	11 March 2011
CN 102055887 A	11 May 2011	US 8407487 B2	26 March 2013
		US 2011107114 A1	05 May 2011
CN 101026822 A	29 August 2007	None	
CN 104486083 A	01 April 2015	None	
CN 1808972 A	26 July 2006	US 7792296 B2	07 September 2010
		US 2006161791 A1	20 July 2006
		US 7477740 B2	13 January 2009
		US 2008310636 A1	18 December 2008
US 2007289012 A1	13 December 2007	None	

国际检索报告

国际申请号

PCT/CN2015/093860

A. 主题的分类

H04L 29/06(2006.01)i; H04N 7/18(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)

H04L, H04N

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))

CNKI, CPRSABS, CNTXT, VEN: 监控, 监视, 网络, 远程, 摄像, 相机, 录像, 图像, 影像, 视频, 隐私, 私密, 敏感, 安全, 认证, 验证, 加密, 隐藏, surveillance, monitor, remote, camera, recorder, image, video, privacy, sensitive, authenticate, authorize, encrypt, hide

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	US 2011057787 A1 (CHUNGHWA TELECOM CO., LTD.) 2011年 3月 10日 (2011 - 03 - 10) 说明书0035-0045段、0050-0055段, 权利要求2, 图1和3	1、10、19
Y	US 2011057787 A1 (CHUNGHWA TELECOM CO., LTD.) 2011年 3月 10日 (2011 - 03 - 10) 同上	2-9、11-18
Y	CN 102055887 A (鸿富锦精密工业深圳有限公司等) 2011年 5月 11日 (2011 - 05 - 11) 说明书2、13-14段, 图2-3	2-6、8-9、11-15、17-18
Y	CN 101026822 A (江苏高通科技实业有限公司) 2007年 8月 29日 (2007 - 08 - 29) 说明书第5页第1行至第6页第15行, 图4	3、7、12、16
PX	CN 104486083 A (小米科技有限责任公司) 2015年 4月 1日 (2015 - 04 - 01) 权利要求1-19	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

2016年 1月 27日

国际检索报告邮寄日期

2016年 2月 25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

授权官员

陈琼

传真号 (86-10)62019451

电话号码 (86-10)62411232

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 1808972 A (国际商业机器公司) 2006年 7月 26日 (2006 - 07 - 26) 说明书第1页第1段、第2页第2段、第3页第2-3段、第6页第3段、第8页第2-3段、第14页第1段至第15页第3段，图1-3	1-19
A	US 2007289012 A1 (LEEMON BAIRD) 2007年 12月 13日 (2007 - 12 - 13) 全文	1-19

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/093860

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)
US	2011057787	A1	2011年 3月 10日	KR	101101855	B1	2012年 1月 5日
				KR	20090023045	A	2009年 3月 4日
				US	8026804	B2	2011年 9月 27日
				TW	200910272	A	2009年 3月 1日
				JP	2009059344	A	2009年 3月 19日
				TW	I338871	B	2011年 3月 11日
CN	102055887	A	2011年 5月 11日	US	8407487	B2	2013年 3月 26日
				US	2011107114	A1	2011年 5月 5日
CN	101026822	A	2007年 8月 29日	无			
CN	104486083	A	2015年 4月 1日	无			
CN	1808972	A	2006年 7月 26日	US	7792296	B2	2010年 9月 7日
				US	2006161791	A1	2006年 7月 20日
				US	7477740	B2	2009年 1月 13日
				US	2008310636	A1	2008年 12月 18日
US	2007289012	A1	2007年 12月 13日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)