

(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 10 月 30 日 (30.10.2014)



(10) 国际公布号
WO 2014/172908 A1

- (51) 国际专利分类号:
G06F 17/30 (2006.01)
- (21) 国际申请号: PCT/CN2013/074865
- (22) 国际申请日: 2013 年 4 月 27 日 (27.04.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 东莞宇龙通信科技有限公司 (DONG-GUAN YULONG TELECOMMUNICATION TECH CO., LTD.) [CN/CN]; 中国广东省东莞市松山湖科技产业园区北部工业城 C 区, Guangdong 523808 (CN)。 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。
- (72) 发明人: 曹坚 (CAO, Jian); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。
- (74) 代理人: 北京友联知识产权代理事务所(普通合伙) (YOULINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路 8 号科技财富中心 A 座 506 室尚志峰, Beijing 100192 (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, IS, JP, KE, KG, KM, 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, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))。

(54) Title: TERMINAL AND METHOD FOR HIDING AND PROTECTING DATA INFORMATION

(54) 发明名称: 终端和数据信息的隐藏保护方法



图 1/ Fig. 1

100 Terminal
102 Information collection unit
104 Information processing unit
106 Information coding unit
108 Information matching unit
110 Information opening unit
112 Information decoding unit
114 Information display unit

(57) Abstract: Provided is a terminal, comprising: an information collection unit which is used for acquiring subsidiary information added for a current image by a user according to an information hiding command received by means of the current image, and collecting authentication information relating to the user; an information processing unit which is used for executing the steps of: eliminating the subsidiary information on the current image, and embedding the subsidiary information and the authentication information in a related manner into a file of the current image from which the subsidiary information is eliminated; or eliminating a display identifier of the subsidiary information on the current image, and embedding the subsidiary information, the display identifier and the authentication information in a related manner into the file of the current image from which the display identifier is eliminated. Also proposed is a method for hiding and protecting data information. By means of the technical solution of the present invention, the subsidiary information in the image can be conveniently and effectively hidden and protected according to user needs, which is beneficial for protecting user privacy and avoiding being peeped by others.

(57) 摘要:

[见续页]

WO 2014/172908 A1

本发明提供了一种终端，包括：信息采集单元，用于根据当前图像接收到的信息隐藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；信息处理单元，用于执行以下步骤：消除所述当前图像上的所述附属信息，并将所述附属信息与所述鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中；或消除所述附属信息在所述当前图像上的显示标识，并将所述附属信息、所述显示标识与所述鉴权信息关联嵌入到消除了所述显示标识的当前图像的文件中。本发明还提出了一种数据信息的隐藏保护方法。通过本发明的技术方案，可以根据用户的需要，方便有效地对图像中的附属信息进行隐藏保护，有利于保护用户隐私，避免他人窥视。

说明书

终端和数据信息的隐藏保护方法

5 技术领域

本发明涉及终端操控技术领域，具体而言，涉及一种终端和一种数据信息的隐藏保护方法。

背景技术

10 为了直观和方便，用户常常直接在感兴趣的图像对象（如人脸、建筑物等）旁边标注其相关信息，如在人脸图像旁边标注其姓名、工作单位、职称和联系电话等。然而用户常常又希望图像上的标注信息不被他人在借用自己手机时查看到，或是当手机丢失后被拾取者查看到。但现有技术中并没有提出较好的方式来隐藏图像上的标注信息等内容，使得用户隐私无法得到保障。

15 因此，本发明提出了一种技术方案可以根据用户的需要，方便有效地对图像中的附属信息进行隐藏保护，有利于保护用户隐私，避免他人窥视。

20 发明内容

本发明正是基于上述问题，提出了一种终端，可以根据用户的需要，方便有效地对图像中的附属信息进行隐藏保护，有利于保护用户隐私，避免他人窥视。

有鉴于此，本发明提出了一种终端，包括：信息采集单元，用于根据
25 当前图像接收到的信息隐藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；信息处理单元，用于执行以下步骤：消除所述当前图像上的所述附属信息，并将所述附属信息与所述鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中；或消除所述附属信息在所述当前图像上的显示标识，并将所述附属信息、所述显示标识

与所述鉴权信息关联嵌入到消除了所述显示标识的当前图像的文件中。

在该技术方案中，通过隐藏图像上的附属信息或附属信息的显示标识，对于非授权用户而言，使其既能够正常查看到图像本身的内容，又无法查看到隐藏了的信息，对于授权用户而言，由于同时嵌入了其鉴权信息，因而可以通过对鉴权信息的识别，从而重新获取和显示出隐藏的信息，实现了提升信息的安全性和对授权用户的隐私性的保护。其中，由于附属信息的类型存在多种可能，因此对于不同的附属信息，由于其自身的特性，可能需要采用不同的处理方式，比如对于一些文字、图形等，可以直接手写、键盘输入等方式添加和显示在当前图像上，则对于这些附属信息，可以直接对其本身进行隐藏等操作；而比如对于一些音频文件、视频文件、文档文件等，其本身就无法直接显示在当前图像上，而是需要通过在当前图像上添加对应的显示标识，然后由用户通过如点击该显示标识，从而调用和显示/播放出相应的附属信息，则对于这些附属信息，需要对其对应的显示标识进行隐藏等操作。当然，具体采用何种显示方式，可以由用户根据实际情况进行设置，然后依据设置结果采用对应的处理方式。

在上述技术方案中，优选地，还包括：信息编码单元，用于将需要嵌入所述文件中的数据信息编码成数字水印，以由所述信息处理单元关联嵌入到所述文件中。

在该技术方案中，通过将需要嵌入所述文件中的数据信息编码成数字水印，可以保证数据信息的安全性以及降低其误检测率，保证数据信息的完整准确。

在上述技术方案中，优选地，所述信息采集单元还用于：获取所述附属信息或所述显示标识在所述当前图像上的位置信息；以及所述信息处理单元还用于：将所述位置信息与所述附属信息或所述显示标识关联嵌入到所述文件中。

在该技术方案中，通过获取所述附属信息或所述显示标识在所述当前图像上的位置信息，可以在重新显示所述附属信息或所述显示标识时确保其所在图像上的位置和消除之前完全一致，这样对于比如图像上存在多个人物的头像，且附属信息为在每个人物旁边标注的名称等信息时，就可以

通过对附属信息的位置恢复，使得每个附属信息与图像上的人物重新对应起来，便于用户的查看。

在上述技术方案中，优选地，所述信息采集单元还用于：根据指定图像接收到的信息激活命令，采集当前操作用户的实时鉴权信息；以及所述
5 终端还包括：信息匹配单元，用于获取所述指定图像的文件中嵌入的鉴权信息，并判断所述鉴权信息与所述实时鉴权信息是否相匹配；其中，所述信息处理单元在所述鉴权信息与所述实时鉴权信息相匹配的情况下，执行下述步骤：获取所述指定图像的文件中嵌入的附属信息，并在所述指定图像上显示所述附属信息；或获取所述指定图像的文件中嵌入的所述附属
10 信息及对应的显示标识，并在所述指定图像上显示出所述显示标识。

在该技术方案中，通过获取图像文件中嵌入的附属信息，可以达到完整还原出原本图像的效果。通过匹配鉴权信息与实时鉴权信息，可以保证隐藏指定图像附属信息的用户与当前查看指定图像附属信息的用户为同一人，或至少为实施“隐藏附属信息”操作的用户授权的其他用户，从而防
15 止图像的附属信息的泄露。

在上述技术方案中，优选地，还包括：信息开启单元，用于当在所述指定图像上显示出所述显示标识时，根据检测到的针对所述显示标识的触摸操作，打开所述显示标识对应的附属信息。

在该技术方案中，通过添加显示标识可以避免在所述鉴权信息与所述
20 实时鉴权信息相匹配的情况下直接自动打开附属信息，有利于让用户控制附属信息打开的时机，使操作更加的人性化，也有利于进一步提升附属信息的使用安全性和对用户的隐私保护。

在上述技术方案中，优选地，还包括：信息解码单元，用于在所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以
25 数字水印的方式嵌入在所述指定图像的文件中的情况下，获取所述指定图像的文件中嵌入的数字水印，并对该数字水印进行解码，以得到对应的信息。

在该技术方案中，针对所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像

的文件中这一情况，通过对数字水印进行解码，得到水印中的鉴权信息和实时鉴权信息进行匹配，在匹配的情况下，还原附属信息或/和显示标识。通过采用数字水印，从而增加了对图像进行暴力破解出其中嵌入的附属信息的难度，有利于提升附属信息的安全性。

- 5 在上述技术方案中，优选地，所述信息采集单元还用于：获取所述指定图像的文件中嵌入的位置信息；所述终端还包括：信息显示单元，用于按照所述位置信息将所述附属信息或所述显示标识显示在所述指定图像上。

10 在该技术方案中，通过获取所述指定图像的文件中嵌入的位置信息，确保所述附属信息或所述显示标识显示在图像上的位置和消除之前完全一致，当附属信息或显示标识与图像中的内容存在一些联系时，比如是对图像内容的解释等，则通过位置恢复有利于用户对图像内容的理解。

在上述技术方案中，优选地，所述信息采集单元采集到的所述附属信息包括以下至少之一或其组合：字符、图形、文件、网址链接。

- 15 在该技术方案中，所述的文件包括以下至少之一或其组合：音频文件、视频文件、图像文件、文档、应用程序。其中，对于不同类型的附属信息，若能够直接显示在图像上，如字符、图形、网址链接等，则直接将附属信息显示在图像上，否则如文件等，则是显示其对应的显示标识。进一步地，假定附属信息为文件 A，则当将文件 A 添加至图像中时，可以通过将该文件 A 直接嵌入图像的文件中，并在图像上创建链接至文件 A 的显示标识，以供用户通过点击显示标识来调用相应的文件 A。
- 20

在上述技术方案中，优选地，所述信息采集单元采集指定用户的鉴权信息的步骤包括以下至少之一或其组合：采集所述指定用户的人脸图像信息、指纹信息、声音信息、视网膜信息，采集所述指定用户输入的密码。

- 25 本发明还提出了一种数据信息的隐藏保护方法，包括：信息采集步骤：根据当前图像接收到的信息隐藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；信息处理步骤：消除所述当前图像上的所述附属信息，并将所述附属信息与所述鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中；或消除所述附属信息在所

述当前图像上的显示标识，并将所述附属信息、所述显示标识与所述鉴权信息关联嵌入到消除了所述显示标识的当前图像的文件中。

在该技术方案中，通过隐藏图像上的附属信息或附属信息的显示标识，对于非授权用户而言，使其既能够正常查看到图像本身的内容，又无法查看到隐藏了的信息，对于授权用户而言，由于同时嵌入了其鉴权信息，因而可以通过对鉴权信息的识别，从而重新获取和显示出隐藏的信息，实现了提升信息的安全性和对授权用户的隐私性的保护。其中，由于附属信息的类型存在多种可能，因此对于不同的附属信息，由于其自身的特性，可能需要采用不同的处理方式，比如对于一些文字、图形等，可以直接手写、键盘输入等方式添加和显示在当前图像上，则对于这些附属信息，可以直接对其本身进行隐藏等操作；而比如对于一些音频文件、视频文件、文档文件等，其本身就无法直接显示在当前图像上，而是需要通过在当前图像上添加对应的显示标识，然后由用户通过如点击该显示标识，从而调用和显示/播放出相应的附属信息，则对于这些附属信息，需要对其对应的显示标识进行隐藏等操作。当然，具体采用何种显示方式，可以由用户根据实际情况进行设置，然后依据设置结果采用对应的处理方式。

在上述技术方案中，优选地，还包括：将需要嵌入所述文件中的数据信息编码成数字水印后，关联嵌入到所述文件中。

在该技术方案中，通过将需要嵌入所述文件中的数据信息编码成数字水印，可以保证数据信息的安全性以及降低其误检测率，保证数据信息的完整准确。

在上述技术方案中，优选地，还包括：获取所述附属信息或所述显示标识在所述当前图像上的位置信息，并将所述位置信息与所述附属信息或所述显示标识关联嵌入到所述文件中。

在该技术方案中，通过获取所述附属信息或所述显示标识在所述当前图像上的位置信息，可以在重新显示所述附属信息或所述显示标识时确保其所在图像上的位置和消除之前完全一致，这样对于比如图像上存在多个人物的头像，且附属信息为在每个人物旁边标注的名称等信息时，就可以通过对附属信息的位置恢复，使得每个附属信息与图像上的人物重新对应

起来，便于用户的查看。

在上述技术方案中，优选地，还包括：根据指定图像接收到的信息激活命令，采集当前操作用户的实时鉴权信息；获取所述指定图像的文件中嵌入的鉴权信息，并在所述鉴权信息与所述实时鉴权信息相匹配的情况下，执行下述步骤：获取所述指定图像的文件中嵌入的附属信息，并在所述指定图像上显示出所述附属信息；或获取所述指定图像的文件中嵌入的所述附属信息及对应的显示标识，并在所述指定图像上显示出所述显示标识。

在该技术方案中，通过获取图像文件中嵌入的附属信息，可以达到完整还原出原本图像的效果。通过匹配鉴权信息与实时鉴权信息，可以保证隐藏指定图像附属信息的用户与当前查看指定图像附属信息的用户为同一人，或至少为实施“隐藏附属信息”操作的用户授权的其他用户，从而防止图像的附属信息的泄露。

在上述技术方案中，优选地，当在所述指定图像上显示出所述显示标识时，还包括：根据检测到的针对所述显示标识的触摸操作，打开所述显示标识对应的附属信息。

在该技术方案中，通过添加显示标识可以避免在所述鉴权信息与所述实时鉴权信息相匹配的情况下直接自动打开附属信息，有利于让用户控制附属信息打开的时机，使操作更加的人性化，也有利于进一步提升附属信息的使用安全性和对用户的隐私保护。

在上述技术方案中，优选地，若所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中，则获取上述信息的步骤包括：获取所述指定图像的文件中嵌入的数字水印，并对该数字水印进行解码，以得到对应的信息。

在该技术方案中，针对所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中这一情况，通过对数字水印进行解码，得到水印中的鉴权信息和实时鉴权信息进行匹配，在匹配的情况下，还原附属信息或/和显示标识。通过采用数字水印，从而增加了对图像进行暴力破解出其中嵌入的附

属信息的难度，有利于提升附属信息的安全性。

在上述技术方案中，优选地，还包括：获取所述指定图像的文件中嵌入的位置信息；按照所述位置信息将所述附属信息或所述显示标识显示在所述指定图像上。

- 5 在该技术方案中，通过获取所述指定图像的文件中嵌入的位置信息，确保所述附属信息或所述显示标识显示在图像上的位置和消除之前完全一致，当附属信息或显示标识与图像中的内容存在一些联系时，比如是对图像内容的解释等，则通过位置恢复有利于用户对图像内容的理解。

- 10 在上述技术方案中，优选地，所述附属信息包括以下至少之一或其组合：字符、图形、文件、网址链接。

- 15 在该技术方案中，所述的文件包括以下至少之一或其组合：音频文件、视频文件、图像文件、文档、应用程序。其中，对于不同类型的附属信息，若能够直接显示在图像上，如字符、图形、网址链接等，则直接将附属信息显示在图像上，否则如文件等，则是显示其对应的显示标识。进一步地，假定附属信息为文件 A，则当将文件 A 添加至图像中时，可以通过将该文件 A 直接嵌入图像的文件中，并在图像上创建链接至文件 A 的显示标识，以供用户通过点击显示标识来调用相应的文件 A。

- 20 在上述技术方案中，优选地，采集指定用户的鉴权信息的步骤包括以下至少之一或其组合：采集所述指定用户的人脸图像信息、指纹信息、声音信息、视网膜信息，采集所述指定用户输入的密码。

通过以上技术方案，可以根据用户的需要，方便有效地对图像中的附属信息进行隐藏保护，有利于保护用户隐私，避免他人窥视。

附图说明

- 25 图 1 示出了根据本发明的实施例的终端的框图；

图 2A 示出了根据本发明的一个实施例的数据信息的隐藏保护方法的流程图；

图 2B 示出了根据本发明的另一个实施例的数据信息的隐藏保护方法的流程图；

图 3 示出了根据本发明的实施例的标注信息的隐藏过程的具体流程图；

图 4 示出了根据本发明的实施例的标注信息的显示过程的具体流程图；

5 图 5A 至图 5F 示出了根据本发明的实施例的数据信息的隐藏保护方法的界面示意图。

具体实施方式

为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

15 图 1 示出了根据本发明的实施例的终端的框图。

如图 1 所示，根据本发明的实施例的终端 100，包括：信息采集单元 102，用于根据当前图像接收到的信息隐藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；信息处理单元 104，用于执行以下步骤：消除所述当前图像上的所述附属信息，并将所述附属信息与所述鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中；或消除所述附属信息在所述当前图像上的显示标识，并将所述附属信息、所述显示标识与所述鉴权信息关联嵌入到消除了所述显示标识的当前图像的文件中。

在该技术方案中，通过隐藏图像上的附属信息或附属信息的显示标识，对于非授权用户而言，使其既能够正常查看到图像本身的内容，又无法查看到隐藏了的信息，对于授权用户而言，由于同时嵌入了其鉴权信息，因而可以通过对鉴权信息的识别，从而重新获取和显示出隐藏的信息，实现了提升信息的安全性和对授权用户的隐私性的保护。其中，由于附属信息的类型存在多种可能，因此对于不同的附属信息，由于其自身的

特性，可能需要采用不同的处理方式，比如对于一些文字、图形等，可以直接手写、键盘输入等方式添加和显示在当前图像上，则对于这些附属信息，可以直接对其本身进行隐藏等操作；而比如对于一些音频文件、视频文件、文档文件等，其本身就无法直接显示在当前图像上，而是需要通过
5 在当前图像上添加对应的显示标识，然后由用户通过如点击该显示标识，从而调用和显示/播放出相应的附属信息，则对于这些附属信息，需要对其对应的显示标识进行隐藏等操作。当然，具体采用何种显示方式，可以由用户根据实际情况进行设置，然后依据设置结果采用对应的处理方式。

在上述技术方案中，优选地，还包括：信息编码单元 106，用于将需
10 要嵌入所述文件中的数据信息编码成数字水印，以由所述信息处理单元关联嵌入到所述文件中。

在该技术方案中，通过将需要嵌入所述文件中的数据信息编码成数字水印，可以保证数据信息的安全性以及降低其误检测率，保证数据信息的完整准确。

15 在上述技术方案中，优选地，所述信息采集单元还用于：获取所述附属信息或所述显示标识在所述当前图像上的位置信息；以及所述信息处理单元还用于：将所述位置信息与所述附属信息或所述显示标识关联嵌入到所述文件中。

在该技术方案中，通过获取所述附属信息或所述显示标识在所述当前
20 图像上的位置信息，可以在重新显示所述附属信息或所述显示标识时确保其所在图像上的位置和消除之前完全一致，这样对于比如图像上存在多个人物的头像，且附属信息为在每个人物旁边标注的名称等信息时，就可以通过对附属信息的位置恢复，使得每个附属信息与图像上的人物重新对应起来，便于用户的查看。

25 在上述技术方案中，优选地，所述信息采集单元还用于：根据指定图像接收到的信息激活命令，采集当前操作用户的实时鉴权信息；以及所述终端还包括：信息匹配单元 108，用于获取所述指定图像的文件中嵌入的鉴权信息，并判断所述鉴权信息与所述实时鉴权信息是否相匹配；其中，所述信息处理单元在所述鉴权信息与所述实时鉴权信息相匹配的情况下，

执行下述步骤：获取所述指定图像的文件中嵌入的附属信息，并在所述指定图像上显示出所述附属信息；或获取所述指定图像的文件中嵌入的所述附属信息及对应的显示标识，并在所述指定图像上显示出所述显示标识。

在该技术方案中，通过获取图像文件中嵌入的附属信息，可以达到完整还原出原本图像的效果。通过匹配鉴权信息与实时鉴权信息，可以保证隐藏指定图像附属信息的用户与当前查看指定图像附属信息的用户为同一人，或至少为实施“隐藏附属信息”操作的用户授权的其他用户，从而防止图像的附属信息的泄露。

在上述技术方案中，优选地，还包括：信息开启单元 110，用于当在所述指定图像上显示出所述显示标识时，根据检测到的针对所述显示标识的触摸操作，打开所述显示标识对应的附属信息。

在该技术方案中，通过添加显示标识可以避免在所述鉴权信息与所述实时鉴权信息相匹配的情况下直接自动打开附属信息，有利于让用户控制附属信息打开的时机，使操作更加的人性化，也有利于进一步提升附属信息的使用安全性和对用户的隐私保护。

在上述技术方案中，优选地，还包括：信息解码单元 112，用于在所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中的情况下，获取所述指定图像的文件中嵌入的数字水印，并对该数字水印进行解码，以得到对应的信息。

在该技术方案中，针对所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中这一情况，通过对数字水印进行解码，得到水印中的鉴权信息和实时鉴权信息进行匹配，在匹配的情况下，还原附属信息或/和显示标识。通过采用数字水印，从而增加了对图像进行暴力破解出其中嵌入的附属信息的难度，有利于提升附属信息的安全性。

在上述技术方案中，优选地，所述信息采集单元还用于：获取所述指定图像的文件中嵌入的位置信息；所述终端还包括：信息显示单元 114，用于按照所述位置信息将所述附属信息或所述显示标识显示在所述指定图

像上。

在该技术方案中，通过获取所述指定图像的文件中嵌入的位置信息，确保所述附属信息或所述显示标识显示在图像上的位置和消除之前完全一致，当附属信息或显示标识与图像中的内容存在一些联系时，比如是对图像内容的解释等，则通过位置恢复有利于用户对图像内容的理解。

在上述技术方案中，优选地，所述信息采集单元采集到的所述附属信息包括以下至少之一或其组合：字符、图形、文件、网址链接。

在该技术方案中，所述的文件包括以下至少之一或其组合：音频文件、视频文件、图像文件、文档、应用程序。其中，对于不同类型的附属信息，若能够直接显示在图像上，如字符、图形、网址链接等，则直接将附属信息显示在图像上，否则如文件等，则是显示其对应的显示标识。进一步地，假定附属信息为文件 A，则当将文件 A 添加至图像中时，可以通过将该文件 A 直接嵌入图像的文件中，并在图像上创建链接至文件 A 的显示标识，以供用户通过点击显示标识来调用相应的文件 A。

在上述技术方案中，优选地，所述信息采集单元采集指定用户的鉴权信息的步骤包括以下至少之一或其组合：采集所述指定用户的人脸图像信息、指纹信息、声音信息、视网膜信息，采集所述指定用户输入的密码。

图 2A 示出了根据本发明的一个实施例的数据信息的隐藏保护方法的流程图。

如图 2A 所示，根据本发明的一个实施例的数据信息的隐藏保护方法，包括：步骤 202A（信息采集步骤）：根据当前图像接收到的信息隐藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；步骤 204A（信息处理步骤）：消除所述当前图像上的所述附属信息，并将所述附属信息与所述鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中。

同时，图 2B 示出了根据本发明的另一个实施例的数据信息的隐藏保护方法的流程图。

如图 2B 所示，根据本发明的另一个实施例的数据信息的隐藏保护方法，包括：步骤 202B（信息采集步骤）：根据当前图像接收到的信息隐

藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；步骤 204B（信息处理步骤）：消除所述附属信息在所述当前图像上的显示标识，并将所述附属信息、所述显示标识与所述鉴权信息关联嵌入到消除了所述显示标识的当前图像的文件中。

5 在图 2A 和图 2B 所示的技术方案中，通过隐藏图像上的附属信息或附属信息的显示标识，对于非授权用户而言，使其既能够正常查看到图像本身的内容，又无法查看到隐藏了的信息，对于授权用户而言，由于同时嵌入了其鉴权信息，因而可以通过对鉴权信息的识别，从而重新获取和显示

10 出隐藏的信息，实现了提升信息的安全性和对授权用户的隐私性的保护。其中，由于附属信息的类型存在多种可能，因此对于不同的附属信息，由于其自身的特性，可能需要采用不同的处理方式，比如对于一些文字、图形等，可以直接手写、键盘输入等方式添加和显示在当前图像上，

15 则对于这些附属信息，可以直接对其本身进行隐藏等操作；而比如对于一些音频文件、视频文件、文档文件等，其本身就无法直接显示在当前图像上，而是需要通过在当前图像上添加对应的显示标识，然后由用户通过如

20 点击该显示标识，从而调用和显示/播放出相应的附属信息，则对于这些附属信息，需要对其对应的显示标识进行隐藏等操作。当然，具体采用何种显示方式，可以由用户根据实际情况进行设置，然后依据设置结果采用对应的处理方式。

20 以下根据图 2A 或图 2B 所示的实施例，详细描述进一步实现的优选实施方式。

 在上述技术方案中，优选地，还包括：将需要嵌入所述文件中的数据信息编码成数字水印后，关联嵌入到所述文件中。

 在该技术方案中，通过将需要嵌入所述文件中的数据信息编码成数字

25 水印，可以保证数据信息的安全性以及降低其误检测率，保证数据信息的完整准确。

 在上述技术方案中，优选地，还包括：获取所述附属信息或所述显示标识在所述当前图像上的位置信息，并将所述位置信息与所述附属信息或所述显示标识关联嵌入到所述文件中。

在该技术方案中，通过获取所述附属信息或所述显示标识在所述当前图像上的位置信息，可以在重新显示所述附属信息或所述显示标识时确保其所在图像上的位置和消除之前完全一致，这样对于比如图像上存在多个人物的头像，且附属信息为在每个人物旁边标注的名称等信息时，就可以
5 通过对附属信息的位置恢复，使得每个附属信息与图像上的人物重新对应起来，便于用户的查看。

在上述技术方案中，优选地，还包括：根据指定图像接收到的信息激活命令，采集当前操作用户的实时鉴权信息；获取所述指定图像的文件中嵌入的鉴权信息，并在所述鉴权信息与所述实时鉴权信息相匹配的情况
10 下，执行下述步骤：获取所述指定图像的文件中嵌入的附属信息，并在所述指定图像上显示出所述附属信息；或获取所述指定图像的文件中嵌入的所述附属信息及对应的显示标识，并在所述指定图像上显示出所述显示标识。

在该技术方案中，通过获取图像文件中嵌入的附属信息，可以达到完
15 整还原出原本图像的效果。通过匹配鉴权信息与实时鉴权信息，可以保证隐藏指定图像附属信息的用户与当前查看指定图像附属信息的用户为同一人，或至少为实施“隐藏附属信息”操作的用户授权的其他用户，从而防止图像的附属信息的泄露。

在上述技术方案中，优选地，当在所述指定图像上显示出所述显示标
20 识时，还包括：根据检测到的针对所述显示标识的触摸操作，打开所述显示标识对应的附属信息。

在该技术方案中，通过添加显示标识可以避免在所述鉴权信息与所述实时鉴权信息相匹配的情况下直接自动打开附属信息，有利于让用户控制附属信息打开的时机，使操作更加的人性化，也有利于进一步提升附属信
25 息的使用安全性和对用户的隐私保护。

在上述技术方案中，优选地，若所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中，则获取上述信息的步骤包括：获取所述指定图像的文件中嵌入的数字水印，并对该数字水印进行解码，以得到对应的信息。

在该技术方案中，针对所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中这一情况，通过对数字水印进行解码，得到水印中的鉴权信息和实时鉴权信息进行匹配，在匹配的情况下，还原附属信息或/和显示标识。通过采用数字水印，从而增加了对图像进行暴力破解出其中嵌入的附属信息的难度，有利于提升附属信息的安全性。

在上述技术方案中，优选地，还包括：获取所述指定图像的文件中嵌入的位置信息；按照所述位置信息将所述附属信息或所述显示标识显示在所述指定图像上。

在该技术方案中，通过获取所述指定图像的文件中嵌入的位置信息，确保所述附属信息或所述显示标识显示在图像上的位置和消除之前完全一致，当附属信息或显示标识与图像中的内容存在一些联系时，比如是对图像内容的解释等，则通过位置恢复有利于用户对图像内容的理解。

在上述技术方案中，优选地，所述附属信息包括以下至少之一或其组合：字符、图形、文件、网址链接。

在该技术方案中，所述的文件包括以下至少之一或其组合：音频文件、视频文件、图像文件、文档、应用程序。其中，对于不同类型的附属信息，若能够直接显示在图像上，如字符、图形、网址链接等，则直接将附属信息显示在图像上，否则如文件等，则是显示其对应的显示标识。进一步地，假定附属信息为文件 A，则当将文件 A 添加至图像中时，可以通过将该文件 A 直接嵌入图像的文件中，并在图像上创建链接至文件 A 的显示标识，以供用户通过点击显示标识来调用相应的文件 A。

在上述技术方案中，优选地，采集指定用户的鉴权信息的步骤包括以下至少之一或其组合：采集所述指定用户的人脸图像信息、指纹信息、声音信息、视网膜信息，采集所述指定用户输入的密码。

图 3 示出了根据本发明的实施例的标注信息的隐藏过程的具体流程图。

如图 3 所示，根据本发明的实施例的标注信息的隐藏过程的具体流程包括：

步骤 302, 打开含标注信息的图像 A, 在此实施例中, 标注信息具体指文本信息, 图像接收的信息隐藏命令具体指用户触屏点击图像, 鉴权信息具体指终端前置摄像头拍摄的人脸图像。

5 步骤 304, 用户触屏点击含标注信息的图像 A, 图像 A 接收到信息隐藏命令。

步骤 306, 通过文本检测获取用户为图像 A 添加的标注附属信息及其所在的区域。

步骤 308, 消除图像 A 上的标注信息得到不含标注信息的图像 B。

步骤 310, 打开前置摄像头, 采集用户相关的鉴权信息。

10 步骤 312, 通过人脸检测, 得到用户的人脸图像 C。

步骤 314, 将标注信息及其所在区域信息还有人脸图像 C 作为水印嵌入到图像 B 中, 得到嵌入水印后的图像 D。图像 D 就是隐藏了标注信息后的图像。

15 与图 3 所示的实施例相应地, 图 4 示出了根据本发明的实施例的标注信息的显示过程的具体流程图。

如图 4 所示, 根据本发明的实施例的标注信息的显示过程的具体流程包括:

20 步骤 402, 打开隐藏标注信息的图像 D, 在此实施例中, 标注信息具体指文本信息, 图像接收的信息显示命令具体指用户触屏点击图像, 鉴权信息具体指终端前置摄像头拍摄的人脸图像。

步骤 404, 用户触屏点击隐藏标注信息的图像 D, 图像 D 接收到信息显示命令。

步骤 406, 打开前置摄像头, 获取实时鉴权图像。

25 步骤 408, 通过人脸检测, 得到用户的人脸图像 C₁, 即为实时鉴权图像。

步骤 410, 提取图像 D 中嵌入的数字水印, 并对该数字水印进行解码。

步骤 412, 通过对数字水印解码得到鉴权图像, 即为隐藏的人脸图像 C。

步骤 414, 判断人脸图像 C_1 和人脸图像 C 是否为同一人的 人脸图像, 若不是, 则执行步骤 416, 若是, 则执行步骤 418。

步骤 416, 在判断人脸图像 C_1 和人脸图像 C 不是同一人的 人脸图像时, 提醒用户无权查看所述图像的标注信息。

5 步骤 418, 在判断人脸图像 C_1 和人脸图像 C 是同一人的 人脸图像时, 从图像 D 的水印信息当中得到标注信息及其所占区域信息, 然后恢复含标注信息的图像 A 。

在图 3 和图 4 的实施例中, 以在图像 A 上添加的是文本形式的标注信息为例进行了描述, 比如用户在图像 A 上某个人物附近标注的联系方式等。当然, 显然也可以在图像 A 上添加其他形式的信息, 比如图形、图像、链接地址等, 且具体的处理方式与文本形式的标注信息相同; 还可以在图像 A 上添加一些文件 (音频、视频、文档等) 等, 但由于文件无法直接显示在图像 A 上, 因而可以在图像 A 上添加相应的显示标识, 则用户可以通过如点击该显示标识, 从而打开相应的文件, 而执行文件的隐藏或显示时, 也是对该显示标识执行隐藏或显示操作。

下面结合图 5A 至图 5F, 对本发明的技术方案进行详细说明, 其中, 图 5A 至图 5F 示出了根据本发明的实施例的数据信息的隐藏保护方法的界面示意图。

如图 5A 所示, 用户通过终端打开图像 502, 其中 “李小明 18987654321” 为图像的附属信息 504。用户需要通过操作隐藏此标注信息, 以避免其他用户查看到。

用户可以通过预设的操作, 比如触屏点击需要执行信息隐藏操作的图像 502, 则终端接收到相应的信息隐藏命令, 如图 5B 所示, 启用前置摄像头并通过人脸识别检测拍下人脸图像 506。

25 此外, 终端还从图 5A 所示的图像 502 中去除附属信息 504, 从而得到所示的不含附属信息 504 的图像 (图中未示出)。

将附属信息 504 及人脸图像 506 作为数字水印嵌入到不含附属信息 504 的图像中, 得到如图 5C 所示的包含但隐藏了附属信息的图像 508, 则对于其他用户而言, 由于处理后的图像 508 仍然能够正常显示, 因而不会

引起注意和怀疑。

如果用户需要查看图像 508 中隐藏的附属信息，则可以采用如触屏点击图像 508，则终端相应地接收到信息显示命令，并如图 5D 所示，打开前置摄像头，通过人脸检测得到用于实时鉴权的当前用户的人脸图像 510。同时，终端提取图像 508 中嵌入的数字水印，并对该数字水印进行解码，得到鉴权图像，即为如图 5B 所示的隐藏的人脸图像 506。

判断人脸图像 506 和当前用户的人脸图像 510 是否为同一人的人脸图像，若不是，则如图 5E 所示，显示提示信息 512，提醒用户无权查看所述图像的标注信息。

10 如果判断人脸图像 506 和当前用户的人脸图像 510 是同一人的人脸图像时，终端继续从图像 508 的水印信息当中得到附属信息 504，然后还原为如图 5A 所示的情形。

当然，如果仅记载附属信息 504，则可能并无法完全恢复至图 5A 所示的情形，而是将附属信息 504 以默认或随意的方式显示出来，那么当图像中存在多个对象时，比如用户不认识的多个人，则可能造成用户难以判断该附属信息 504 具体对应的对象。因此，可以通过记录附属信息 504 在图像 502 上的位置信息，并与附属信息 504、人脸图像 506 一并嵌入不含附属信息 504 的图像中，从而当用户从图像 508 中提取出嵌入的数字水印后，可以据此将附属信息 504 恢复至初始位置。

20 此外，由于附属信息 504 为文字信息，可以直接显示在图像 502 上，但对于一些如音频文件、视频文件等，无法直接显示在图像 502 上，则如图 5F 所示，比如将某个音频文件添加至图像 502 时，则一方面将该音频文件嵌入图像 502 的文件中，另一方面可以在图像 502 上显示出对应的显示标识 514，从而用户可以通过该显示标识 514 打开相应的音频文件。

25 同时，当用户需要执行类似上述的隐藏/显示操作时，则直接对显示标识 514 进行隐藏/显示，而对于用户的人脸图像的采集、信息的嵌入等则与上述过程类似，此处不再赘述。

以上结合附图详细说明了本发明的技术方案，考虑到在现有技术中，用户通过对图像加密来防止图像的附属信息不被别人偷窥，而加密和解密

需要用户记得并输入密码，如此繁杂的过程不利于用户的操作。因此，本发明提出了一种终端和一种数据信息的隐藏保护方法，可以根据用户的需要，方便有效地对图像中的附属信息进行隐藏保护，有利于保护用户隐私，避免他人窥视。

- 5 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种终端，其特征在于，包括：

信息采集单元，用于根据当前图像接收到的信息隐藏命令，获取用户
5 为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；

信息处理单元，用于执行以下步骤：

消除所述当前图像上的所述附属信息，并将所述附属信息与所述
鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中；

或消除所述附属信息在所述当前图像上的显示标识，并将所述附
10 属信息、所述显示标识与所述鉴权信息关联嵌入到消除了所述显示标
识的当前图像的文件中。

2. 根据权利要求 1 所述的终端，其特征在于，还包括：

信息编码单元，用于将需要嵌入所述文件中的数据信息编码成数字水
印，以由所述信息处理单元关联嵌入到所述文件中。

15 3. 根据权利要求 1 所述的终端，其特征在于，

所述信息采集单元还用于：获取所述附属信息或所述显示标识在所述
当前图像上的位置信息；以及

所述信息处理单元还用于：将所述位置信息与所述附属信息或所述显
示标识关联嵌入到所述文件中。

20 4. 根据权利要求 1 所述的终端，其特征在于，所述信息采集单元还
用于：根据指定图像接收到的信息激活命令，采集当前操作用户的实时鉴
权信息；以及

所述终端还包括：

信息匹配单元，用于获取所述指定图像的文件中嵌入的鉴权信息，并
25 判断所述鉴权信息与所述实时鉴权信息是否相匹配；

其中，所述信息处理单元在所述鉴权信息与所述实时鉴权信息相匹配
的情况下，执行下述步骤：

获取所述指定图像的文件中嵌入的附属信息，并在所述指定图像
上显示出所述附属信息；

或获取所述指定图像的文件中嵌入的所述附属信息及对应的显示标识，并在所述指定图像上显示出所述显示标识。

5. 根据权利要求 4 所述的终端，其特征在于，还包括：

信息开启单元，用于当在所述指定图像上显示出所述显示标识时，根据检测到的针对所述显示标识的触摸操作，打开所述显示标识对应的附属信息。

6. 根据权利要求 4 所述的终端，其特征在于，还包括：

信息解码单元，用于在所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中的情况下，获取所述指定图像的文件中嵌入的数字水印，并对该数字水印进行解码，以得到对应的信息。

7. 根据权利要求 4 所述的终端，其特征在于，所述信息采集单元还用于：获取所述指定图像的文件中嵌入的位置信息；

所述终端还包括：

15 信息显示单元，用于按照所述位置信息将所述附属信息或所述显示标识显示在所述指定图像上。

8. 根据权利要求 1 至 7 中任一项所述的终端，其特征在于，所述信息采集单元采集到的所述附属信息包括以下至少之一或其组合：

字符、图形、图像、音频文件、视频文件、网址链接。

20 9. 根据权利要求 1 至 7 中任一项所述的终端，其特征在于，所述信息采集单元采集指定用户的鉴权信息的步骤包括以下至少之一或其组合：

采集所述指定用户的人脸图像信息、指纹信息、声音信息、视网膜信息，采集所述指定用户输入的密码。

10. 一种数据信息的隐藏保护方法，其特征在于，包括：

25 信息采集步骤：

根据当前图像接收到的信息隐藏命令，获取用户为所述当前图像添加的附属信息，并采集与所述用户相关的鉴权信息；

信息处理步骤：

30 消除所述当前图像上的所述附属信息，并将所述附属信息与所述鉴权信息关联嵌入到消除了所述附属信息的当前图像的文件中；

或消除所述附属信息在所述当前图像上的显示标识，并将所述附属信息、所述显示标识与所述鉴权信息关联嵌入到消除了所述显示标识的当前图像的文件中。

11. 根据权利要求 10 所述的数据信息的隐藏保护方法，其特征在于，还包括：

将需要嵌入所述文件中的数据信息编码成数字水印后，关联嵌入到所述文件中。

12. 根据权利要求 10 所述的数据信息的隐藏保护方法，其特征在于，还包括：

10 获取所述附属信息或所述显示标识在所述当前图像上的位置信息，并将所述位置信息与所述附属信息或所述显示标识关联嵌入到所述文件中。

13. 根据权利要求 10 所述的数据信息的隐藏保护方法，其特征在于，还包括：

15 根据指定图像接收到的信息激活命令，采集当前操作用户的实时鉴权信息；

获取所述指定图像的文件中嵌入的鉴权信息，并在所述鉴权信息与所述实时鉴权信息相匹配的情况下，执行下述步骤：

获取所述指定图像的文件中嵌入的附属信息，并在所述指定图像上显示出所述附属信息；

20 或获取所述指定图像的文件中嵌入的所述附属信息及对应的显示标识，并在所述指定图像上显示出所述显示标识。

14. 根据权利要求 13 所述的数据信息的隐藏保护方法，其特征在于，当在所述指定图像上显示出所述显示标识时，还包括：

25 根据检测到的针对所述显示标识的触摸操作，打开所述显示标识对应的附属信息。

15. 根据权利要求 13 所述的数据信息的隐藏保护方法，其特征在于，若所述鉴权信息和所述附属信息或所述鉴权信息、所述附属信息和所述显示标识以数字水印的方式嵌入在所述指定图像的文件中，则获取上述信息的步骤包括：

获取所述指定图像的文件中嵌入的数字水印，并对该数字水印进行解码，以得到对应的信息。

16. 根据权利要求 13 所述的数据信息的隐藏保护方法，其特征在于，还包括：

5 获取所述指定图像的文件中嵌入的位置信息；

按照所述位置信息将所述附属信息或所述显示标识显示在所述指定图像上。

17. 根据权利要求 10 至 16 中任一项所述的数据信息的隐藏保护方法，其特征在于，所述附属信息包括以下至少之一或其组合：

10 字符、图形、文件、网址链接。

18. 根据权利要求 10 至 16 中任一项所述的数据信息的隐藏保护方法，其特征在于，采集指定用户的鉴权信息的步骤包括以下至少之一或其组合：

15 采集所述指定用户的人脸图像信息、指纹信息、声音信息、视网膜信息，采集所述指定用户输入的密码。

说明书附图



图 1

5

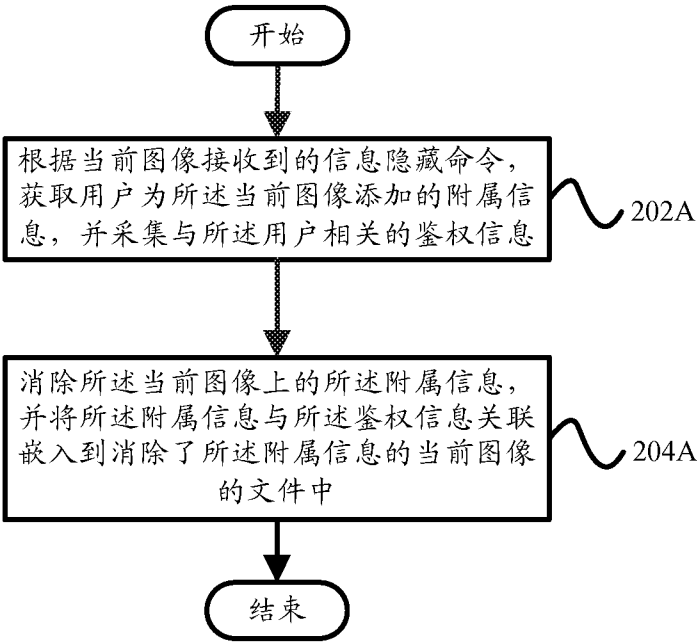


图 2A

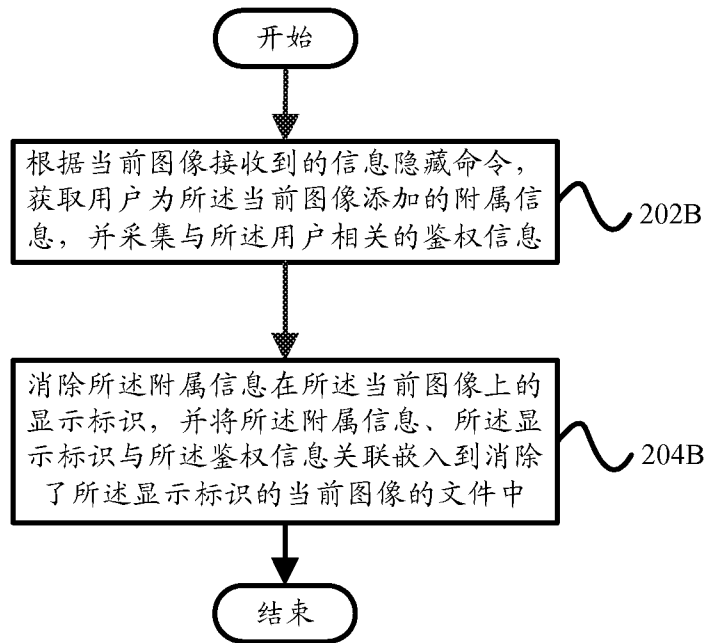


图 2B

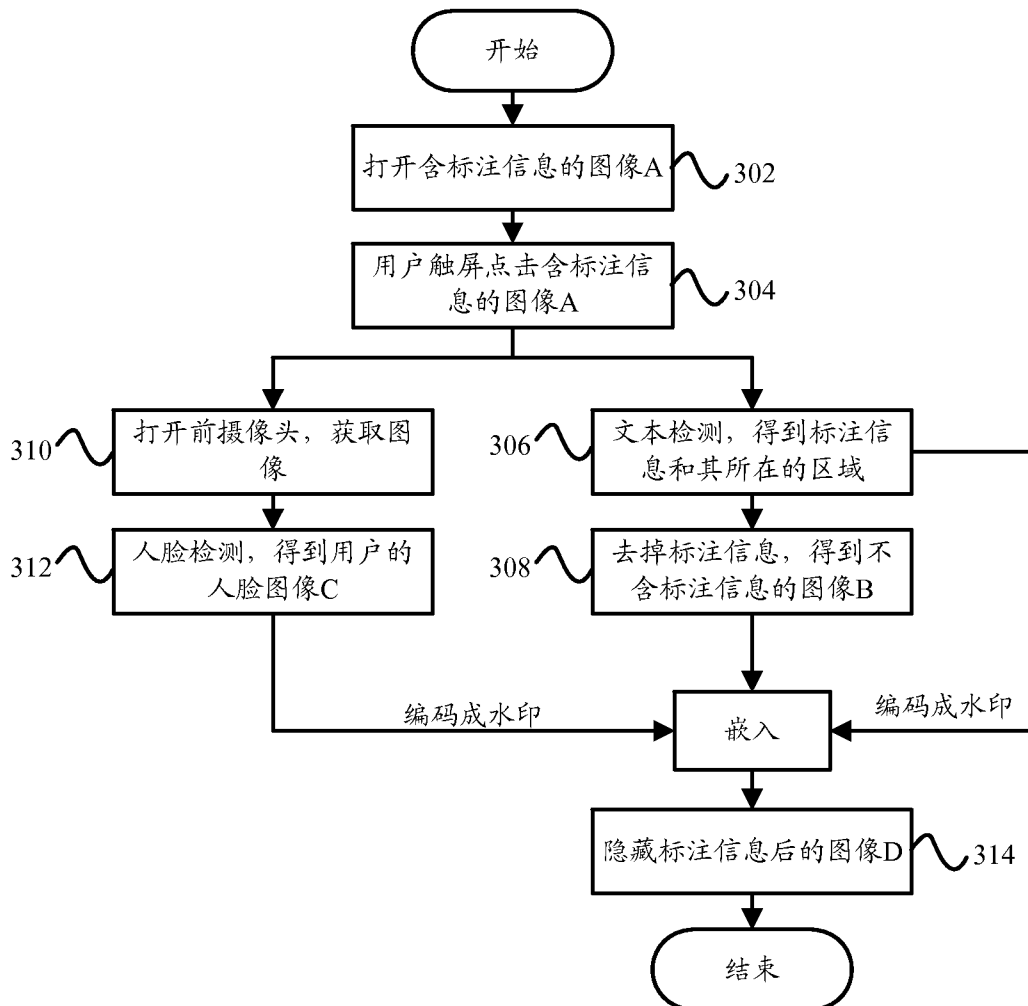


图 3

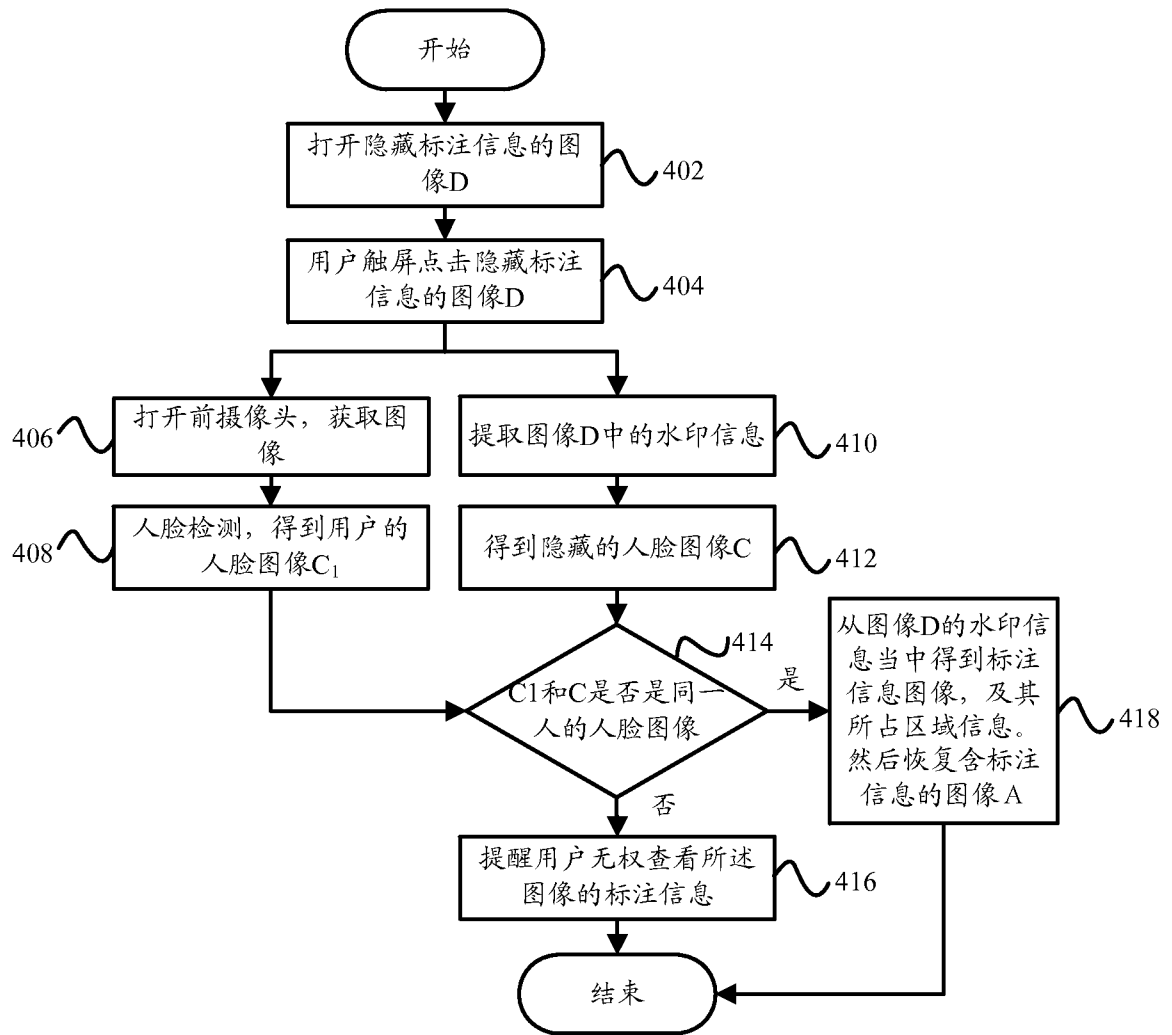


图 4

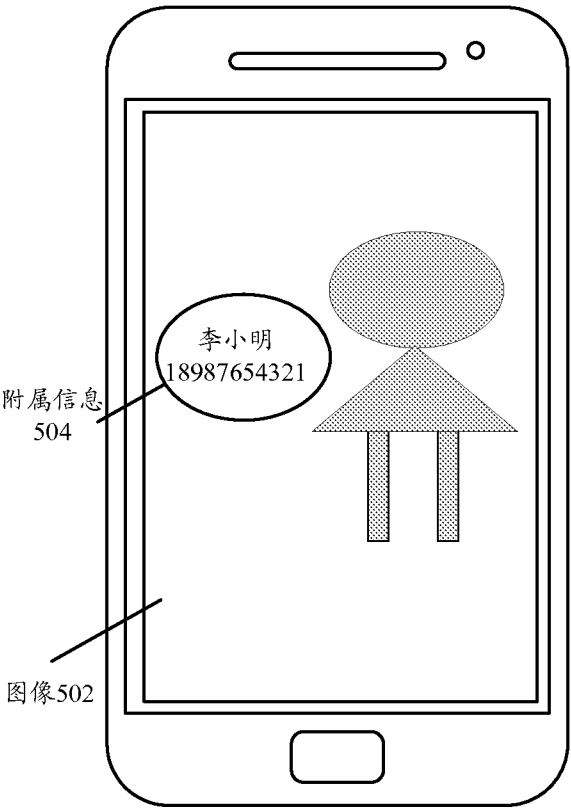


图 5A

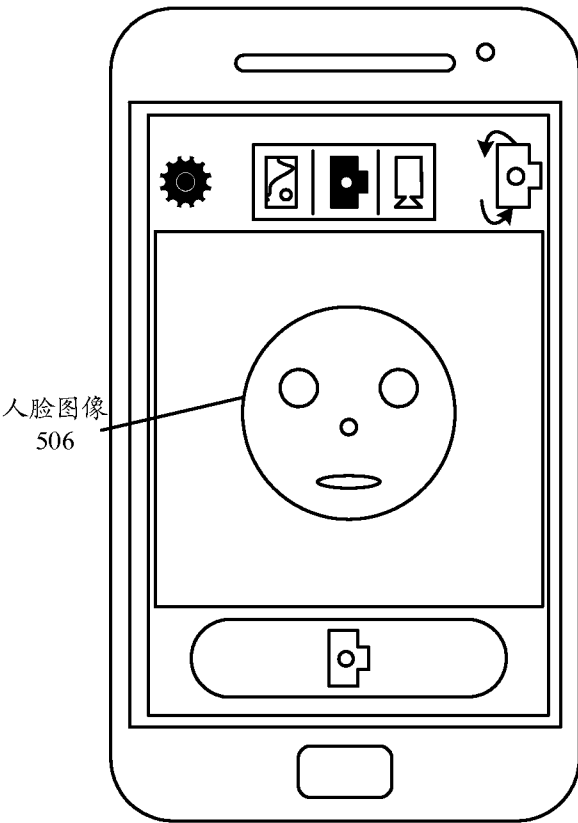


图 5B

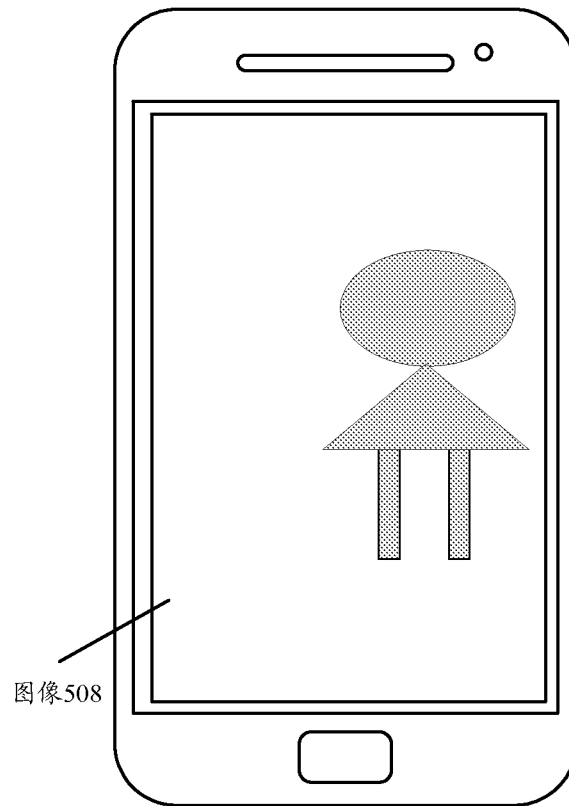


图 5C

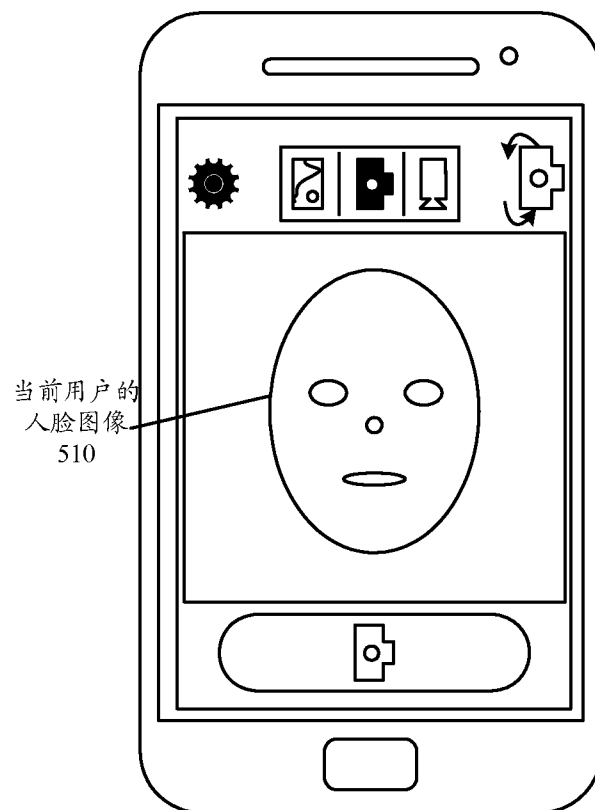


图 5D

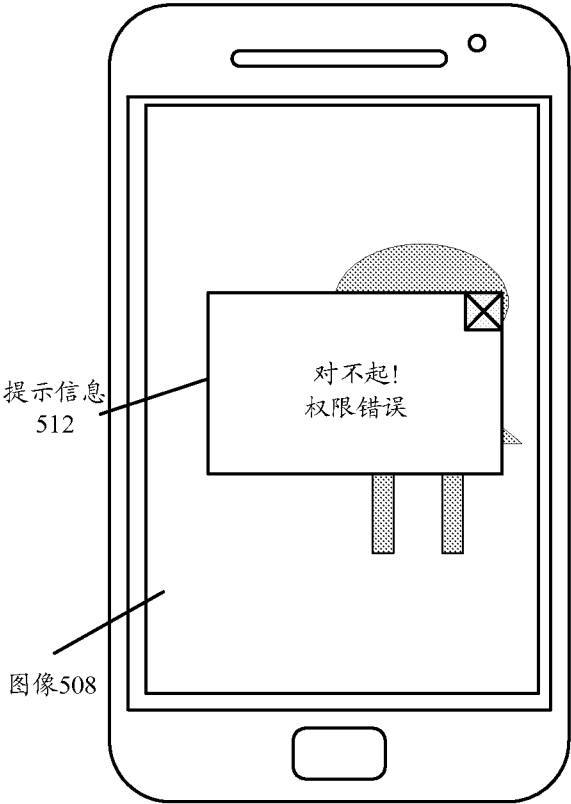


图 5E

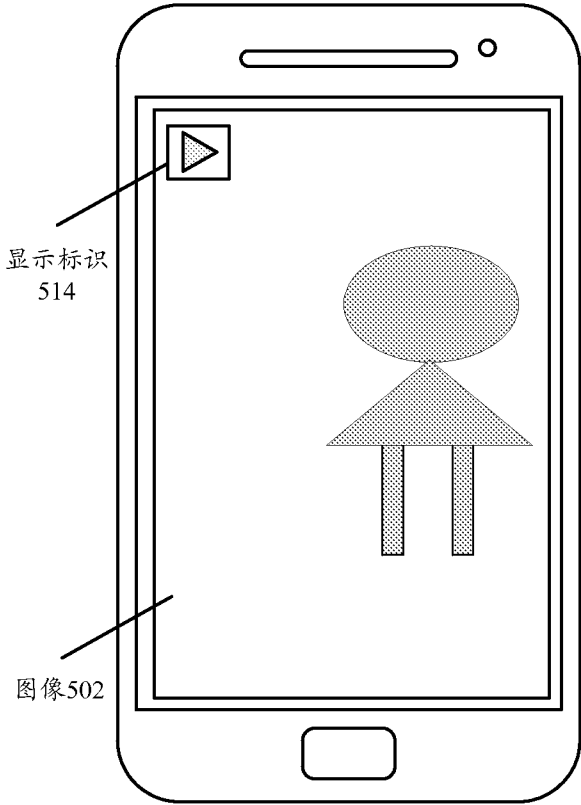


图 5F

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/074865

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/30 (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)

IPC: 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, WPI, EPODOC, IEEE, GOOGLE: note, comment, annotation, label, hide, conceal, image, terminal, mobile, PDA, phone, additional information, eliminate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101120358 A (AMAZON TECHNOLOGIES INC.) 06 February 2008 (06.02.2008) description, page 9, lines 4-26, page 10, line 1 to page 11, line 19, and page 13, line 24 to page 14, line 17	1-18
A	CN 101997969 A (SONY ERICSSON MOBILE COMMUNICATION AB) 30 March 2011 (30.03.2011) the whole document	1-18
A	CN 101082912 A (SHANGHAI JIETU SOFTWARE TECHNOLOGY CO., LTD.) 05 December 2007 (05.12.2007) the whole document	1-18
A	US 2009204555 A1 (NEC LABORATORIES AMERICA, INC.) 13 August 2009 (13.08.2009) the whole document	1-18

☐ 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 02 January 2014 (02.01.2014)	Date of mailing of the international search report 20 February 2014 (20.02.2014)
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 OUYANG, Qi Telephone No. (86-10) 62413658

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/074865

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101120358 A	06.02.2008	US 2006161578 A1	20.07.2006
		WO 2006078728 A2	27.07.2006
		EP 1842150 A2	10.10.2007
		JP 2008527580 A	24.07.2008
		CA 2594573 A1	27.07.2006
		US 2008168073 A1	10.07.2008
		US 2011184828 A1	28.07.2011
CN 101997969 A	30.03.2011	WO 2011019467 A1	17.02.2011
		US 2011039598 A1	17.02.2011
CN 101082912 A	05.12.2007	WO 2007124664 A1	08.11.2007
		CN 101082766 A	05.12.2007
		CN 101090460 A	19.12.2007
		US 2009116764 A1	07.05.2009
US 2009204555 A1	13.08.2009	None	

A. 主题的分类

G06F 17/30 (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)

IPC: 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, WPI, EPODOC, IEEE, GOOGLE: 注释, 解释, 标注, 注解, 附属信息, 隐藏, 消除, 隐蔽, 终端, 移动, 手机, note, comment, annotation, label, hide, conceal, image, terminal, mobile, PDA, phone

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 101120358 A (亚马逊科技公司) 06.2 月 2008 (06.02.2008) 说明书第 9 页第 4-26 行, 第 10 页第 1 行-第 11 页第 19 行, 第 13 页第 24 行-第 14 页第 17 行	1-18
A	CN 101997969 A (索尼爱立信移动通讯有限公司) 30.3 月 2011 (30.03.2011) 全文	1-18
A	CN 101082912 A (上海杰图软件技术有限公司) 05.12 月 2007 (05.12.2007) 全文	1-18
A	US 2009204555 A1 (NEC LABORATORIES AMERICA, INC.) 13.8 月 2009 (13.08.2009) 全文	1-18

☐ 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

02.1 月 2014 (02.01.2014)

国际检索报告邮寄日期

20.2 月 2014 (20.02.2014)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

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

欧阳琦

电话号码: (86-10) 62413658

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/074865

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 101120358 A	06.02.2008	US 2006161578 A1	20.07.2006
		WO 2006078728 A2	27.07.2006
		EP 1842150 A2	10.10.2007
		JP 2008527580 A	24.07.2008
		CA 2594573 A1	27.07.2006
		US 2008168073 A1	10.07.2008
		US 2011184828 A1	28.07.2011
CN 101997969 A	30.03.2011	WO 2011019467 A1	17.02.2011
CN 101082912 A	05.12.2007	US 2011039598 A1	17.02.2011
		WO 2007124664 A1	08.11.2007
		CN 101082766 A	05.12.2007
		CN 101090460 A	19.12.2007
US 2009204555 A1	13.08.2009	US 2009116764 A1	07.05.2009
		无	