201734877

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201734877 A

(43)公開日： 中華民國 106 (2017) 年 10 月 01 日

(21)申請案號：106102211 (22)申請日： 中華民國 106 (2017) 年 01 月 20 日

(51)Int. Cl.： *G06F21/60 (2013.01)* *G06F9/44 (2006.01)*

(30)優先權：2016/03/29 中國大陸 201610188604.2

(71)申請人：阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)

香港

(72)發明人：呂晨晨 (CN)；管維剛 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：16 項 圖式數：3 共 25 頁

(54)名稱

基於應用程序的用戶資訊的隱藏方法及裝置

(57)摘要

本發明揭示了一種基於應用程序的用戶資訊的隱藏方法及裝置。該方法包括：獲取應用程序內媒體文件的屬性列表的操作權限；讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內；將所述媒體文件重新保存。通過將應用程序內產生的用戶資訊寫入應用程序的媒體文件的屬性列表內，如此用戶資訊得到隱藏，在行動終端本地文件夾內不易被找到和獲取，從而達到防止產生應用程序內的用戶資訊被洩露目的。

指定代表圖：

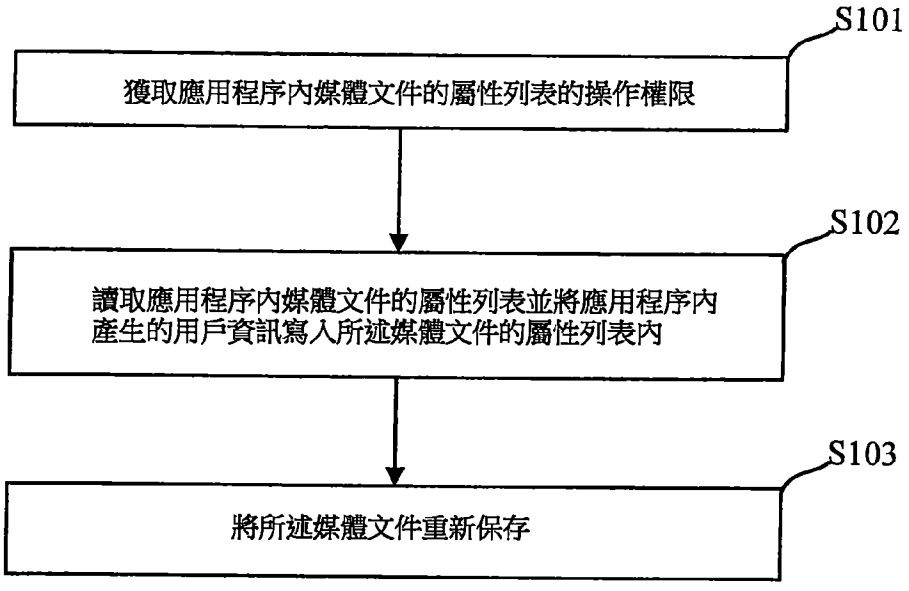

圖 1

201734877

發明摘要

※申請案號：106102211

※申請日：106年01月20日　　※IPC分類：G06F 21/60 (2013.01)
G06F 9/44 (2006.01)

【發明名稱】(中文/英文)

基於應用程序的用戶資訊的隱藏方法及裝置

【中文】

本發明揭示了一種基於應用程序的用戶資訊的隱藏方法及裝置。該方法包括：獲取應用程序內媒體文件的屬性列表的操作權限；讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內；將所述媒體文件重新保存。通過將應用程序內產生的用戶資訊寫入應用程序的媒體文件的屬性列表內，如此用戶資訊得到隱藏，在行動終端本地文件夾內不易被找到和獲取，從而達到防止產生應用程序內的用戶資訊被洩露目的。

【英文】

【代表圖】

【本案指定代表圖】：第(１)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

基於應用程序的用戶資訊的隱藏方法及裝置

【技術領域】

本發明涉及終端技術領域，尤其涉及一種基於應用程序的用戶資訊的隱藏方法及裝置。

【先前技術】

在各種無線行動終端以及移動互聯網飛速發展的時境下，越來越多的無線行動終端被應用於人們的日常生活中，很多無線行動終端已發展成為生活中的一部分。目前不論是 iOS、Android 還是 Windows 系統，資料傳播的快速性、方便性、穩定性和安全性已經成為衡量一個無線行動終端的重要指標，尤其在涉及到用戶重要、私有資訊時，安全性更是重中之重。

在無線行動終端中使用應用程序可以實現購物、聊天、交友、出行等各種生活、工作功能，極大地方便用戶。使用應用程序過程中，應用程序會產生各種資料，如應用程序登錄的帳號、密碼，以及如聊天記錄、購物的訂單資訊、支付資訊等涉及敏感、機密的用戶資訊。這些用戶資訊一般以文本文件及資料庫文件的形式保存於行動終端本地文件夾內，因此，上述文本文件及資料庫文件容易

被查找到從而容易導致用戶資訊的洩露。為了防止用戶資訊輕易洩露，應用程序運行中產生的敏感、機密的用戶資訊會預先進行加密後再儲存在行動終端本地文件夾內。然而，雖然上述資訊已經被加密，但是加密的資訊密文串還是完全暴露在外邊，比如，可以通過目前比較常見的第三方工具（itools、豌豆莢等資料庫工具）查到文本文件及資料庫文件（如.txt、.db、.plist 等文件），從而獲取這些加密後的資訊，這樣增加了對敏感、機密資訊被破解機率，導致敏感、機密的用戶資訊洩露，安全性較低。

【發明內容】

本發明實施例提供一種基於應用程序的用戶資訊的隱藏方法及裝置，用以解決現有技術中在應用程序運行過程中產生的用戶資訊容易被發現和獲取，而導致用戶資訊洩露的問題。

本發明實施例提供一種基於應用程序的用戶資訊的隱藏方法，其包括：

獲取應用程序內媒體文件的屬性列表的操作權限；

讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內；

將所述媒體文件重新保存。

進一步的，所述用戶資訊包括敏感或機密的資訊。

進一步的，所述獲取應用程序內媒體文件的屬性列表的操作權限，具體包括：

獲取應用程序內媒體文件的句柄；

通過媒體文件的句柄，來獲取應用程序內媒體文件的屬性列表的讀取、寫入權限。

進一步的，所述將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內，具體包括：

將應用程序內產生的用戶資訊以鍵值對的形式寫入所述媒體文件的屬性列表內。

進一步的，所述媒體文件包括照片、音頻及視頻文件。

進一步的，所述用戶資訊為加密過的用戶資訊。

本發明實施例還提供了一種基於應用程序的用戶資訊的隱藏方法，其包括：

獲取應用程序內媒體文件的屬性列表的操作權限；

對應用程序內產生的用戶資訊進行邏輯處理；

讀取應用程序內媒體文件的屬性列表並將應用程序內經過邏輯處理的用戶資訊寫入所述媒體文件的屬性列表內；

將所述媒體文件重新保存。

進一步的，所述用戶資訊包括敏感或機密的資訊。

進一步的，所述獲取應用程序內媒體文件的屬性列表的操作權限，具體包括：

獲取應用程序內媒體文件的句柄；

通過媒體文件的句柄，來獲取應用程序內媒體文件的屬性列表的讀取、寫入權限。

進一步的，所述將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內，具體包括：

將應用程序內產生的用戶資訊以鍵值對的形式寫入所述媒體文件的屬性列表內。

進一步的，所述媒體文件包括照片、音頻及視頻文件。

進一步的，所述用戶資訊為加密過的用戶資訊。

進一步的，所述對應用程序內產生的用戶資訊進行邏輯處理，具體包括：

對應用程序內產生的用戶資訊進行可逆的邏輯處理。

進一步的，所述對應用程序內產生的用戶資訊進行邏輯處理，具體包括：

通過對稱加密算法，對應用程序內產生的用戶資訊進行對稱加密處理。

本發明實施例還提供了一種基於應用程序的用戶資訊的隱藏裝置，其包括：

獲取模組，用於獲取應用程序內媒體文件的屬性列表的操作權限；

讀寫模組，用於讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內；

保存模組，用於將所述媒體文件重新保存。

進一步的，所述裝置還包括：

邏輯處理模組，用於對應用程序內產生的用戶資訊進

行邏輯處理。

與現有技術相比，本發明實施例提供的一種基於應用程序的用戶資訊的隱藏方法及裝置，通過將應用程序內產生的用戶資訊寫入應用程序的媒體文件的屬性列表內，如此用戶資訊得到隱藏，在行動終端本地文件夾內不易被找到和獲取，從而達到防止產生應用程序內的用戶資訊被洩露目的。

【圖式簡單說明】

此處所說明的附圖用來提供對本發明的進一步理解，構成本發明的一部分，本發明的示意性實施例及其說明用於解釋本發明，並不構成對本發明的不當限定。在附圖中：

圖 1 為本發明實施例一提供的基於應用程序的用戶資訊的隱藏方法的流程示意圖；

圖 2 為本發明實施例二提供的基於應用程序的用戶資訊的隱藏方法的流程示意圖；

圖 3 為本發明實施例三提供的基於應用程序的用戶資訊的隱藏裝置的結構示意圖。

【實施方式】

為使本發明的目的、技術方案和優點更加清楚，下面將結合本發明具體實施例及相應的附圖對本發明技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本發

明一部分實施例，而不是全部的實施例。基於本發明中的實施例，本領域普通技術人員在沒有做出創造性勞動前提下所獲得的所有其他實施例，都屬於本發明保護的範圍。

圖 1 為本發明實施例提供的基於應用程序的用戶資訊的隱藏方法的流程示意圖。下面將結合圖 1 對本發明實施例提供的基於應用程序的用戶資訊的隱藏的方法進行詳細介紹，如圖 1 所示，本發明實施例提供的基於應用程序的用戶資訊的隱藏的方法包括以下步驟。

步驟 S101：獲取應用程序內媒體文件的屬性列表的操作權限。

在本發明實施例中，行動終端應用程序在運行過程中，會產生與用戶操作對應的用戶資訊，該用戶資訊包括涉及用戶敏感、機密的資訊，上述用戶資訊自動保存至行動終端本地。上述應用程序可以為各類安裝於行動終端的應用程序，如支付類、交友類應用程序。以支付類應用程序為例，用戶在使用、操作支付類應用程序的過程中，會產生登錄帳號、登錄密碼、身份證號、手機號、銀行卡號及支付密碼等敏感、機密的用戶資訊。上述用戶資訊中，如登陸密碼、支付密碼為機密的用戶資訊，登陸帳號、身份證、手機號、銀行卡號為敏感資訊。

進一步的，應用程序在運行過程中，不同的業務類型或應用場景對應不同的用戶資訊。繼續以支付類應用程序為例，在支付的應用場景下，會產生包括與支付相關的敏感、機密的用戶資訊。另外，在好友聊天的應用場景下，

又會產生涉及聊天資訊的用戶資訊。

在本步驟中，應用程序內的媒體文件可以位於應用程序的安裝目錄下，可以作為用於保存上述用戶資訊的載體。不同類型的用戶資訊可以保存於不同的媒體文件內。進一步的，上述用戶資訊可以保存於媒體文件的屬性列表內，屬性列表內包括用於描述媒體文件資訊的屬性資訊。上述媒體文件可以為圖片、音頻及視頻文件中的任意一種。較佳地，上述媒體文件可以為圖片文件。上述媒體文件可以作為用於應用程序圖面顯示的一部分預先打包至應用程序安裝包內，當應用程序安裝後，上述媒體文件就位於應用程序的安裝目錄下。

用戶可以通過鼠標針移動到媒體文件，按鼠標右鍵，將鼠標通過點擊媒體文件屬性選項，再點擊詳細資訊就可以看到關於媒體文件的一個屬性列表，其內包括屬性標識及對應的屬性值。比如，在照片的屬性列表內，包括名稱、項目類型、創建日期、修改日期等在內的屬性標識及屬性標識對應的屬性值。

進一步的，獲取應用程序內媒體文件的屬性列表的操作權限，具體包括：

獲取應用程序內媒體文件的句柄；通過所述媒體文件的句柄，來獲取應用程序內媒體文件的屬性列表的讀取、寫入權限。

媒體文件的句柄（file handle）也可以稱為媒體文件的對象指針。句柄是指使用的一個唯一的整數值，即一個

4 字節(64 位程序中為 8 字節)長的數值，來標識應用程序中的不同對象和同類中的不同的實例。通過獲取到的媒體文件的句柄，應用程序可使用這對句柄對媒體文件，即媒體文件的屬性列表進行讀取、寫入資訊的操作。

步驟 S102：讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內。

在本實施例中，由於獲取了媒體文件的句柄，因此媒體文件的屬性列表可以作為一個可進行讀寫操作的對象。媒體文件的屬性列表內包括用於描述媒體文件的屬性資訊。

上述媒體文件的屬性列表被讀取至行動終端的隨機存取記憶體中，並在行動終端的隨機存取記憶體中將上述用戶資訊寫入媒體文件的屬性列表內。

上述將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內，具體包括：

將應用程序內產生的用戶資訊以鍵值對的形式寫入所述媒體文件的屬性列表內。

在應用程序運行過程中會產生了與用戶操作相關的用戶資訊，如敏感資訊、機密資訊等。該用戶資訊可以是未經加密的明文，該用戶資訊可以直接寫入媒體文件的屬性列表內。

比如，在應用程序運行過程中，產生了帳戶密碼，其保存於本地。為了避免用戶的帳戶密碼被盜取，該帳戶密

碼可以以鍵值對（Key-Value）的形式寫入媒體文件的屬性列表內，以便隱藏該帳戶密碼資訊。具體的，帳戶密碼對應的屬性標識 Key 可以被命名為 Password，帳戶密碼的屬性值 Value 可以為一串代表密碼的文字，該串文字可以為明文。當然，為了更好地隱藏及偽裝帳戶密碼，帳戶密碼對應的屬性標識 Key 可以設置為系統類的屬性標識 Key，如此更不易被識別。

另外，需要說明的是，應用程序內產生的與用戶操作相關的用戶資訊也可以為是已經加密的密文。針對用戶資訊的加密方法包括：MD5，DES，RSA，SM2，SM3 等加密算法。

進一步的，不同應用場景下的產生的用戶資訊可以寫入不同的媒體文件內。比如，在應用程序支付場景產生的用戶資訊（如支付密碼、訂單資訊等）可以寫入一個媒體文件中，如圖片 a 中；在聊天應用場景下產生的用戶資訊（如聊天資訊內的電話號碼、銀行卡號等）可以寫入另一個媒體文件中，如圖片 b 中。

步驟 S103：將所述媒體文件重新保存。

在本實施例中，當需要進行隱藏的用戶資訊均寫入媒體文件的屬性列表內後，將上述媒體文件重新保存。當用戶後續通過鼠標針移動到該媒體文件，按鼠標右鍵，將鼠標通過點擊媒體文件屬性選項，再點擊詳細資訊就可以看到寫入屬性列表內的用戶資訊已存於所述媒體文件的屬性列表內了。

具體地，若媒體文件保存成功，則該媒體文件保存於應用程序的安裝路徑下，此時用戶資訊偽裝成功。

若媒體文件保存失敗，則可每隔一個預設時間段（如 3 至 5 秒）自動重新保存，預設重新保存的次數可以是 3 次。若在 3 次重新保存的機會內媒體文件保存成功，則表示用戶資訊的偽裝成功。若重新保存超過 3 次後，媒體文件仍未保存成功，則將這次保存失敗保存至失敗隊列中。

當應用程序內再次產生涉及敏感、機密資訊的用戶資訊時，用戶資訊寫入媒體文件並且媒體文件成功保存後，自動調用失敗隊列，重新保存媒體文件直到其成功保存，如果還是保存失敗，則將這次任務重新加入新的失敗隊列，重複上述過程直到媒體文件保存成功為止。

圖 2 為本發明實施二例提供的基於應用程序的用戶資訊的隱藏的方法流程示意圖。下面將結合圖 2 對本發明實施例二提供的基於應用程序的用戶資訊的隱藏的方法進行詳細介紹，如圖 2 所示，本發明實施例二提供的基於應用程序的用戶資訊的隱藏的方法包括以下步驟。

步驟 S201：獲取應用程序內媒體文件的屬性列表的操作權限。

在本實施例中，此步驟與本發明實施例一提供的基於應用程序的用戶資訊的隱藏方法的步驟 S101 基本相同，此處不再贅述。

步驟 S202：對應用程序內產生的用戶資訊進行邏輯處理。

在本實施例中，為了防止產生於應用程序內的用戶資訊（如敏感、機密的用戶資訊）輕易洩露，需要對應用程序內的上述用戶資訊預先進行邏輯處理。需要說明的是，上述邏輯處理為可逆的邏輯處理，即針對用戶資訊的邏輯處理過程可逆。

對應用程序內產生的用戶資訊進行邏輯處理，具體包括：

通過對稱加密算法，對應用程序內產生的用戶資訊進行對稱加密處理。

當然，需要說明的是，該用戶資訊在邏輯處理前也可以通過 MD5，DES，RSA，SM2，SM3 等加密算法進行一次加密處理。

步驟 S203：讀取應用程序內媒體文件的屬性列表並將應用程序內經過邏輯處理的用戶資訊寫入所述媒體文件的屬性列表內。

需要說明的是，在本實施例中，經過邏輯處理後的用戶資訊也可以以鍵值對（Key-Value）的形式寫入媒體文件的屬性列表內，以便隱藏該用戶資訊。以用戶資訊為帳戶密碼為例，帳戶密碼對應的屬性標識 Key 可以被命名為 Password，帳戶密碼的屬性值 Value 可以為一串邏輯處理後的文字或字符串。

步驟 S204：將所述媒體文件重新保存。

在本實施例中，當需要進行隱藏的用戶資訊均寫入媒體文件的屬性列表內後，將上述媒體文件重新保存。此步

驟與本發明實施例一提供的基於應用程序的用戶資訊的隱藏方法的步驟 S103 基本相同，此處不再贅述。

以上為本發明實施例提供的基於應用程序的用戶資訊的隱藏方法，基於同樣的思路，本發明實施例三還提供了基於應用程序的用戶資訊的隱藏裝置。參見圖 3，該圖示出了本發明實施例三提供的基於應用程序的用戶資訊的隱藏裝置的結構，其具體包括：

獲取模組 301，用於獲取應用程序內媒體文件的屬性列表的操作權限；

邏輯處理模組 302，用於對應用程序內產生的用戶資訊進行邏輯處理；

讀寫模組 303，用於讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊或經過邏輯處裡的用戶資訊寫入媒體文件的屬性列表內；

保存模組 304，用於將媒體文件重新保存。

需要說明的是，上述用屬性列表內包括描述媒體文件的屬性資訊。戶資訊為敏感、機密的資訊，上述媒體文件包括照片、音頻及視頻文件。另外，上述用戶資訊也可以為預先加密過的用戶資訊。

針對應用程序內產生的用戶資訊進行邏輯處理為可逆的邏輯處理，比如，該邏輯處理可以為對稱加密。

綜上所述，本發明實施例提供的一種基於應用程序的用戶資訊的隱藏方法及裝置，通過將應用程序內產生的用戶資訊寫入應用程序的媒體文件的屬性列表內，如此用戶

資訊得到隱藏，在行動終端本地文件夾內不易被找到和獲取，從而達到防止產生應用程序內的用戶資訊被洩露目的。

在 20 世紀 90 年代，對於一個技術的改進可以很明顯地區分是硬體上的改進（例如，對二極管、晶體管、開關等電路結構的改進）還是軟體上的改進（對於方法流程的改進）。然而，隨著技術的發展，當今的很多方法流程的改進已經可以視為硬體電路結構的直接改進。設計人員幾乎都通過將改進的方法流程編程到硬體電路中來得到相應的硬體電路結構。因此，不能說一個方法流程的改進就不能用硬體實體模組來實現。例如，可編程邏輯器件（Programmable Logic Device, PLD）（例如現場可編程門陣列（Field Programmable Gate Array，FPGA））就是這樣一種積體電路，其邏輯功能由用戶對器件編程來確定。由設計人員自行編程來把一個數字系統“整合”在一片 PLD 上，而不需要請晶片製造廠商來設計和製作專用的積體電路晶片 2。而且，如今，取代手工地製作積體電路晶片，這種編程也多半改用“邏輯編譯器（logic compiler）”軟體來實現，其與程序開發撰寫時所用的軟體編譯器相類似，而要編譯之前的原始代碼也得用特定的編程語言來撰寫，此稱之為硬體描述語言（Hardware Description Language，HDL），而 HDL 也並非僅有一種，而是有許多種，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）與 Verilog2。本領域技術人員也應該清楚，只需要將方法流程用上述幾種硬體描述語言稍作邏輯編程並編程到積體電路中，就可以很容易得到實現該邏輯方法流程的硬體電路。

控制器可以按任何適當的方式實現，例如，控制器可以採取例如微處理器或處理器以及儲存可由該（微）處理器執行的計算機可讀程序代碼（例如軟體或韌體）的計算機可讀媒體、邏輯門、開關、專用積體電路（Application Specific Integrated Circuit，ASIC）、可編程邏輯控制器和嵌入微控制器的形式，控制器的例子包括但不限於以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，儲存器控制器還可以被實現為儲存器的控制邏輯的一部分。本領域技術人員也知道，除了以純計算機可讀程序代碼方式實現控制器以外，完全可以通過將方法步驟進行邏輯編程來使得控制器以邏輯門、開關、專用積體電路、可編程邏輯控制器和嵌入微控制器等的形式來實現相同功能。因此這種控制器可以被認為是一種硬體部件，而對其內包括的用於

實現各種功能的裝置也可以視為硬體部件內的結構。或者甚至，可以將用於實現各種功能的裝置視為既可以是實現方法的軟體模組又可以是硬體部件內的結構。

上述實施例闡明的系統、裝置、模組或單元，具體可以由計算機晶片或實體實現，或者由具有某種功能的產品來實現。

為了描述的方便，描述以上裝置時以功能分為各種單元分別描述。當然，在實施本發明時可以把各單元的功能在同一個或多個軟體和/或硬體中實現。

本領域內的技術人員應明白，本發明的實施例可提供為方法、系統、或計算機程序產品。因此，本發明可採用完全硬體實施例、完全軟體實施例、或結合軟體和硬體方面的實施例的形式。而且，本發明可採用在一個或多個其中包含有計算機可用程序代碼的計算機可用儲存媒體（包括但不限於磁盤儲存器、CD-ROM、光學儲存器等）上實施的計算機程序產品的形式。

本發明是參照根據本發明實施例的方法、設備（系統）、和計算機程序產品的流程圖和／或方框圖來描述的。應理解可由計算機程序指令實現流程圖和／或方框圖中的每一流程和／或方框、以及流程圖和／或方框圖中的流程和／或方框的結合。可提供這些計算機程序指令到通用計算機、專用計算機、嵌入式處理機或其他可編程資料處理設備的處理器以產生一個機器，使得通過計算機或其他可編程資料處理設備的處理器執行的指令產生用於實現

在流程圖一個流程或多個流程和／或方框圖一個方框或多個方框中指定的功能的裝置。

這些計算機程序指令也可儲存在能引導計算機或其他可編程資料處理設備以特定方式工作的計算機可讀儲存器中，使得儲存在該計算機可讀儲存器中的指令產生包括指令裝置的製造品，該指令裝置實現在流程圖一個流程或多個流程和／或方框圖一個方框或多個方框中指定的功能。

這些計算機程序指令也可裝載到計算機或其他可編程資料處理設備上，使得在計算機或其他可編程設備上執行一系列操作步驟以產生計算機實現的處理，從而在計算機或其他可編程設備上執行的指令提供用於實現在流程圖一個流程或多個流程和／或方框圖一個方框或多個方框中指定的功能的步驟。

在一個典型的配置中，計算設備包括一個或多個處理器(CPU)、輸入/輸出介面、網路介面和隨機存取記憶體。

隨機存取記憶體可能包括計算機可讀媒體中的非永久性儲存器，隨機存取儲存器 (RAM) 和/或非易失性隨機存取記憶體等形式，如唯讀儲存器 (ROM) 或閃存(flash RAM)。隨機存取記憶體是計算機可讀媒體的示例。

計算機可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是計算機可讀指令、資料結構、程序的模組或其他資料。計算機的儲存媒體的例子包括，但不限於相變隨機存取記憶體 (PRAM)、靜態隨機存取儲存器 (SRAM)、動態

隨機存取儲存器 (DRAM)、其他類型的隨機存取儲存器(RAM)、唯讀儲存器 (ROM)、電可擦除可編程唯讀儲存器 (EEPROM)、快閃記憶體或其他隨機存取記憶體技術、唯讀光碟唯讀儲存器 (CD-ROM)、數字多功能光碟 (DVD)或其他光學儲存、磁盒式磁帶，磁帶磁盤儲存或其他磁性儲存設備或任何其他非傳輸媒體，可用於儲存可以被計算設備訪問的資訊。按照本文中的界定，計算機可讀媒體不包括暫存電腦可讀媒體(transitory media)，如調製的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

本領域技術人員應明白，本發明的實施例可提供為方法、系統或計算機程序產品。因此，本發明可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本發明可採用在一個或多個其中包含有計算機可用程序代碼的計算機可用儲存媒體（包括但不限於磁盤儲存器、CD-ROM、光學儲存器等）上實施的計算機程序產品的形式。

本發明可以在由計算機執行的計算機可執行指令的一般上下文中描述，例如程序模組。一般地，程序模組包括執行特定任務或實現特定抽象資料類型的例程、程序、對象、組件、資料結構等等。也可以在分布式計算環境中實踐本發明，在這些分布式計算環境中，由通過通信網路而被連接的遠程處理設備來執行任務。在分布式計算環境中，程序模組可以位於包括儲存設備在內的本地和遠程計算機儲存媒體中。

本說明書中的各個實施例均採用遞進的方式描述，各個實施例之間相同相似的部分互相參見即可，每個實施例重點說明的都是與其他實施例的不同之處。尤其，對於系統實施例而言，由於其基本相似於方法實施例，所以描述的比較簡單，相關之處參見方法實施例的部分說明即可。

以上所述僅為本發明的實施例而已，並不用於限制本發明。對於本領域技術人員來說，本發明可以有各種更改和變化。凡在本發明的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本發明的申請專利範圍之內。

【符號說明】

301：獲取模組

302：邏輯處理模組

303：讀寫模組

304：保存模組

申請專利範圍

1. 一種基於應用程序的用戶資訊的隱藏方法，包括：

獲取應用程序內媒體文件的屬性列表的操作權限；

讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內；

將所述媒體文件重新保存。

2. 如申請專利範圍第 1 項所述的方法，其中，所述用戶資訊包括敏感或機密的資訊。

3. 如申請專利範圍第 1 項所述的方法，其中，所述獲取應用程序內媒體文件的屬性列表的操作權限，具體包括：

獲取應用程序內媒體文件的句柄；

通過媒體文件的句柄，來獲取應用程序內媒體文件的屬性列表的讀取、寫入權限。

4. 如申請專利範圍第 1 項所述的方法，其中，所述將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內，具體包括：

將應用程序內產生的用戶資訊以鍵值對的形式寫入所述媒體文件的屬性列表內。

5. 如申請專利範圍第 1 項所述的方法，其中，所述媒體文件包括照片、音頻及視頻文件。

6. 如申請專利範圍第 1 項所述的方法，其中，所述用戶資訊為加密過的用戶資訊。

7. 一種基於應用程序的用戶資訊的隱藏方法，其中，其包括：

獲取應用程序內媒體文件的屬性列表的操作權限；

對應用程序內產生的用戶資訊進行邏輯處理；

讀取應用程序內媒體文件的屬性列表並將應用程序內經過邏輯處理的用戶資訊寫入所述媒體文件的屬性列表內；

將所述媒體文件重新保存。

8. 如申請專利範圍第 7 項所述的方法，其中，所述用戶資訊包括敏感或機密的資訊。

9. 如申請專利範圍第 7 項所述的方法，其中，所述獲取應用程序內媒體文件的屬性列表的操作權限，具體包括：

獲取應用程序內媒體文件的句柄；

通過媒體文件的句柄，來獲取應用程序內媒體文件的屬性列表的讀取、寫入權限。

10. 如申請專利範圍第 7 項所述的方法，其中，所述將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內，包括：

將應用程序內產生的用戶資訊以鍵值對的形式寫入所述媒體文件的屬性列表內。

11. 如申請專利範圍第 7 項所述的方法，其中，所述媒體文件包括照片、音頻及視頻文件。

12. 如申請專利範圍第 7 項所述的方法，其中，所述

用戶資訊為加密過的用戶資訊。

13. 如申請專利範圍第 7 項所述的方法，其中，所述對應用程序內產生的用戶資訊進行邏輯處理，包括：

對應用程序內產生的用戶資訊進行可逆的邏輯處理。

14. 如申請專利範圍第 7 項所述的方法，其特徵在於，所述對應用程序內產生的用戶資訊進行邏輯處理，包括：

通過對稱加密算法，對應用程序內產生的用戶資訊進行對稱加密處理。

15. 一種基於應用程序的用戶資訊的隱藏裝置，其中，其包括：

獲取模組，用於獲取應用程序內媒體文件的屬性列表的操作權限；

讀寫模組，用於讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內；

保存模組，用於將所述媒體文件重新保存。

16. 如申請專利範圍第 15 項所述的裝置，其中，所述裝置還包括：

邏輯處理模組，用於對應用程序內產生的用戶資訊進行邏輯處理。

圖式

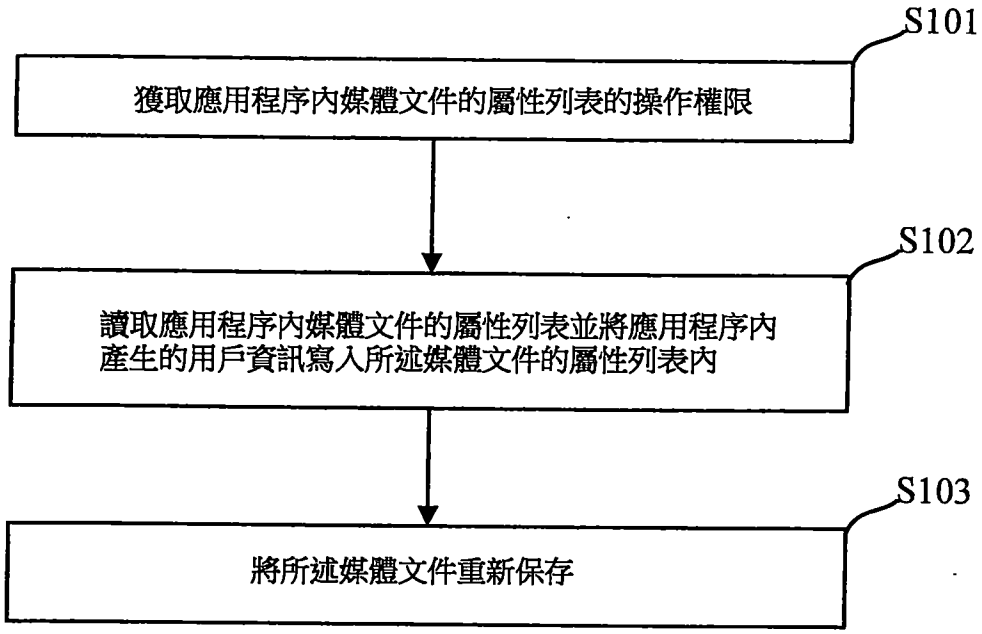
S101
獲取應用程序內媒體文件的屬性列表的操作權限
S102
讀取應用程序內媒體文件的屬性列表並將應用程序內產生的用戶資訊寫入所述媒體文件的屬性列表內
S103
將所述媒體文件重新保存

圖 1

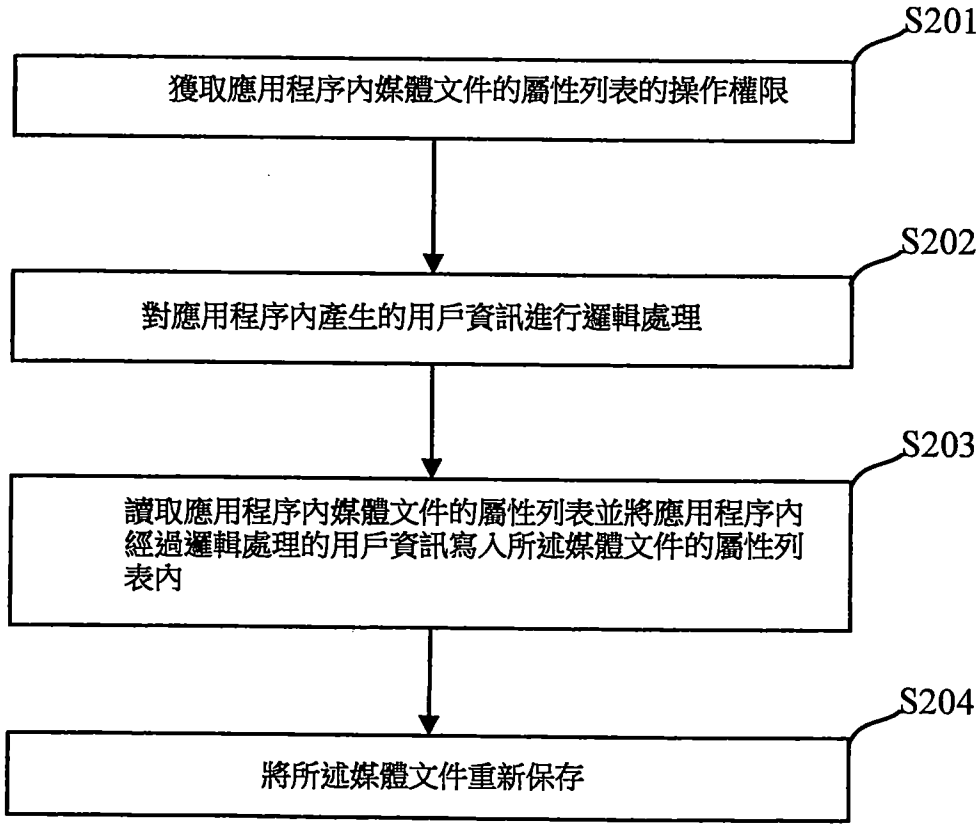
S201
獲取應用程序內媒體文件的屬性列表的操作權限
S202
對應用程序內產生的用戶資訊進行邏輯處理
S203
讀取應用程序內媒體文件的屬性列表並將應用程序內經過邏輯處理的用戶資訊寫入所述媒體文件的屬性列表內
S204
將所述媒體文件重新保存

圖 2

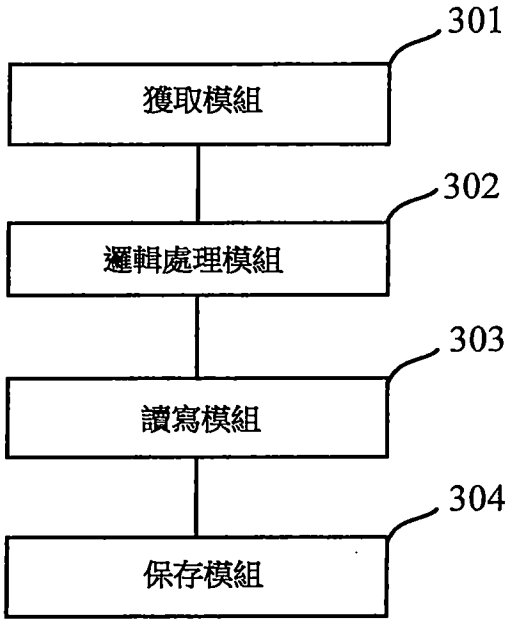

圖 3