



(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I529556 B

(45)公告日：中華民國 105 (2016) 年 04 月 11 日

(21)申請案號：101145762

(22)申請日：中華民國 101 (2012) 年 12 月 05 日

(51)Int. Cl. : G06F21/32 (2013.01)

G06K9/36 (2006.01)

H04L9/32 (2006.01)

(30)優先權：2012/08/13

中國大陸

201210285041.0

(71)申請人：王國芳 (香港地區) WONG, KWOK FONG (HK)

香港

(72)發明人：王國芳 (CN)；程佩儀 (CN)

(74)代理人：黃靜雯

(56)參考文獻：

TW 201227527A

TW 201227527A1

CN 101316169A

CN 101330386A

審查人員：李國福

申請專利範圍項數：11 項 圖式數：3 共 16 頁

(54)名稱

身份認證管理裝置及其方法

(57)摘要

本發明為一種身份認證管理裝置，包括用戶端以及後臺。用戶端包括終端設備以及指紋感測器，指紋感測器包括用於採集指紋資訊的採集識別裝置以及用於存儲包括指紋資訊以及該指紋資訊相對應用戶的用戶資訊的記憶體，終端設備用於登記或識別指紋感測器採集到的指紋資訊。後臺包括與終端設備相交互連接的身份認證伺服器以及與身份認證伺服器相交互連接的多個應用管理區，應用管理區中包括應用單元以及應用資訊，當指紋資訊被終端設備登記或認可後，身份認證伺服器將與指紋資訊相對應的用戶資訊進行生成或核對，並進入該用戶的應用管理區，在應用管理區中，可對應用單元或應用資訊進行操作。

指定代表圖：

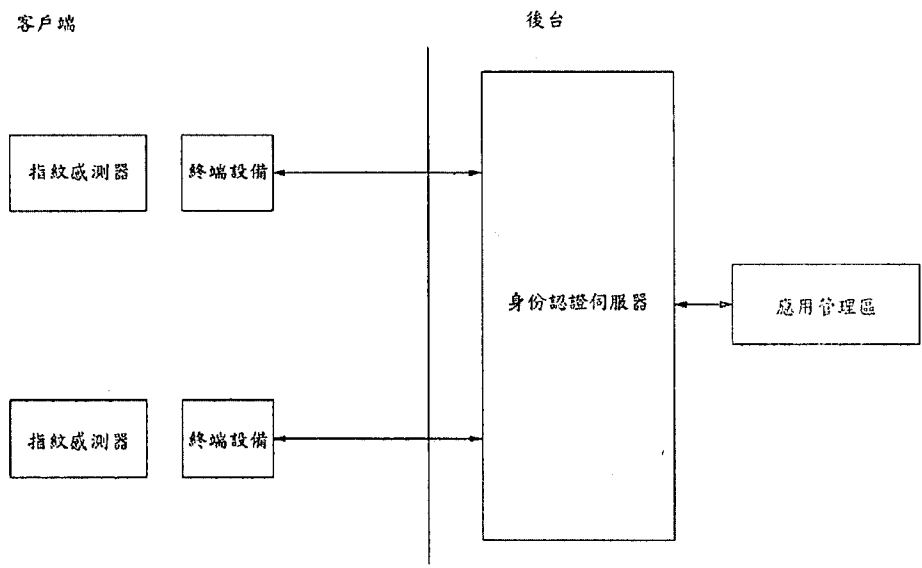


圖1



申請日: 101. 12. 5

IPC分類: G06F 21/32 (2013.01)
G06K 9/36 (2006.01)
H04L 9/32 (2006.01)

【發明摘要】

【中文發明名稱】 身份認證管理裝置及其方法

【中文】

本發明為一種身份認證管理裝置，包括用戶端以及後臺。用戶端包括終端設備以及指紋感測器，指紋感測器包括用於採集指紋資訊的採集識別裝置以及用於存儲包括指紋資訊以及該指紋資訊相對應用戶的用戶資訊的記憶體，終端設備用於登記或識別指紋感測器採集到的指紋資訊。後臺包括與終端設備相交互連接的身份認證伺服器以及與身份認證伺服器相交互連接的多個應用管理區，應用管理區中包括應用單元以及應用資訊，當指紋資訊被終端設備登記或認可後，身份認證伺服器將與指紋資訊相對應的用戶資訊進行生成或核對，並進入該用戶的應用管理區，在應用管理區中，可對應用單元或應用資訊進行操作。

【指定代表圖】 圖1

【特徵化學式】

無

【發明說明書】

【中文發明名稱】 身份認證管理裝置及其方法

【技術領域】

【0001】 本發明涉及一種身份認證管理裝置及其方法。

【先前技術】

【0002】 隨著互聯網的快速發展，網路在人們的生活中扮演著越來越重要的角色，流覽網頁，使用各種應用，幾乎是生活的一部分；目前，我們對經常訪問的網站或者經常使用的應用，會使用收藏夾進行管理，以方便快捷訪問；但是收藏夾僅僅是保存網站鏈結，點擊後快速進入的是網站，其他的用戶登錄等操作均是在連結網站上進行的。甚至有些平臺把用戶經常訪問的網站進行記憶管理，以方便用戶選擇。但是這樣有個缺點，就是任何訪問本機的人都可以看到，對於用戶而言，缺少私密性，安全性也不高。那怎樣才能對這些網站鏈結和各種應用進行集中管理，並且集中管理其用戶登錄等資訊，真正安全快捷的使用網路鏈結及應用，確保用戶的私密性，是我們目前要解決的。

【發明內容】

【0003】 本發明提供一種身份認證管理裝置，包括：

【0004】 用戶端，用戶端包括多個終端設備以及分別與每個終端設備相互連接的指紋感測器，指紋感測器包括用於採集指紋資訊的採集識別裝置以及用於存儲包括指紋資訊以及該指紋資訊相對應用戶的用戶資訊的記憶體，終端設備用於登記或識別指紋感測器採集

到的指紋資訊；

- 【0005】 後臺，後臺包括與終端設備相交互連接的身份認證伺服器以及與身份認證伺服器相交互連接的多個應用管理區，應用管理區中包括應用單元以及應用資訊，當指紋資訊被終端設備登記或認可後，身份認證伺服器將與指紋資訊相對應的用戶資訊進行生成或核對，並進入該用戶的應用管理區，在應用管理區中，可對應用單元或應用資訊進行操作。
- 【0006】 在上述身份認證管理裝置之中，身份認證伺服器包括用於辨別用戶身份的用户認證單元以及用於存放註冊後的用户資訊的用户檔案管理單元。
- 【0007】 在上述身份認證管理裝置之中，終端設備與身份認證伺服器、身份認證伺服器與應用伺服器通過網路相交互連接。
- 【0008】 在上述身份認證管理裝置之中，應用管理區中的應用單元包括但不局限於遊戲、郵件、網站中的一種或幾種。
- 【0009】 在上述身份認證管理裝置之中，應用管理區中的應用資訊包括但不局限於用戶名、密碼中的一種或幾種。
- 【0010】 在上述身份認證管理裝置之中，所述的應用管理區中的應用單元包括好友管理單元，該好友管理單元可通過交換指紋資訊管理好友以及對於好友之間的操作。
- 【0011】 在上述身份認證管理裝置之中，所述的應用管理區中的應用單元包括聊天單元，所述用戶端上設置有用於解密或加密聊天單元中的聊天資訊的聊天軟體。

- 【0012】 一種身份認證及管理方法，包括以下步驟：
- 【0013】 採集指紋資訊，通過指紋感測器的採集識別裝置提取用戶的指紋資訊；
- 【0014】 指紋資訊的登記或識別階段，終端設備將採集到的指紋資訊進行登記或識別；
- 【0015】 用戶認證階段，後臺的身份認證伺服器將新登記的指紋資訊生成新的用戶資訊或將與指紋資訊相對的用戶資訊進行核對；
- 【0016】 應用管理階段，在應用管理區中，用戶可對應用單元或應用資訊進行操作。
- 【0017】 在上述身份認證及管理方法之中，指紋感測器的採集識別裝置提取用戶的指紋資訊，終端設備將採集到的與指紋資訊相對的用戶資訊進行核對指紋資訊進行登記，後臺的身份認證伺服器的用戶認證單元將新登記的指紋資訊生成新的用戶，並將該用戶資訊保存在身份認證伺服器的用戶檔案管理單元。
- 【0018】 在上述身份認證及管理方法之中，指紋感測器的採集識別裝置提取用戶的指紋資訊，終端設備將採集到的指紋資訊進行識別，後臺的身份認證伺服器的用戶認證單元將存儲在用戶檔案管理單元中的用戶資訊與指紋資訊相對的用戶資訊進行核對。
- 【0019】 在上述身份認證及管理方法之中，用戶可對應用單元或應用資訊進行操作為刪除、添加或修改中的一種或幾種。
- 【0020】 本發明採用以上結構或方法具有以下有益效果：
- 【0021】 1、在這個平臺上，用戶的身份是要通過指紋驗證才能夠進入應

用管理區，在此基礎上就保證了用戶的私密性；

【0022】 2、用戶登記的時候，配以相對應的指紋感測器，而且相關的用戶資訊存儲在指紋感測器上，增加了用戶的安全性，減少了指紋傳感設備或者帳號遺失後對用戶資料的影響；

【0023】 3、利用指紋資訊統一管理用戶自定義的網站及其他相關應用，同時管理自定義網站以及其他應用的帳號以及密碼，使用戶能夠通過掃描指定指紋而快捷準確的登錄相關網站或者其他應用，並完成相應的帳戶登錄，節省了用戶時間的同時，也減少了在不同網站重複進行帳號登錄的麻煩，並且大大提高了安全性；

【0024】 4、具有好友添加以及好友對話功能，在未經解密的情況下，第三方無法看到私聊資訊。

【圖式簡單說明】

【0026】 附圖1為本發明中的結構示意圖。

【0027】 附圖2為本發明中的新用戶的操作流程圖。

【0028】 附圖3為本發明中的老用戶的操作流程圖。

【實施方式】

【0029】 下面結合附圖對本發明的較佳實施例進行詳細闡述，以使本發明的優點和特徵能更易於被本領域技術人員理解，從而對本發明的保護範圍做出更為清楚明確的界定。

【0030】 如附圖2和3所示，本發明的第一實施例中，一種身份認證及管理方法，包括以下步驟：

【0031】 A) 採集指紋資訊，通過指紋感測器的採集識別裝置提取用戶的

指紋資訊；

- 【0032】 B) 指紋資訊的登記或識別階段可以分爲登記和識別兩個階段，
- 【0033】 B1) 指紋資訊的登記，對於新的用戶指紋感測器的採集識別裝置提取用戶的指紋資訊，終端設備將採集到的與指紋資訊相對的用戶資訊進行核對指紋資訊進行登記。
- 【0034】 B2) 指紋資訊的識別，對於完成登記認證過的用戶：指紋感測器的採集識別裝置提取用戶的指紋資訊，終端設備將採集到的指紋資訊進行識別。
- 【0035】 C) 用戶認證階段是通過後臺的身份認證伺服器將進行生成或核對用戶資訊；
- 【0036】 C1) 對於新用戶，後臺的身份認證伺服器的用戶認證單元將新登記的指紋資訊生成新的用戶，並將該用戶資訊保存在身份認證伺服器的用戶檔案管理單元。
- 【0037】 C2) 對於完成登記認證過的用戶，後臺的身份認證伺服器的用戶認證單元將存儲在用戶檔案管理單元中的用戶資訊與指紋資訊相對的用戶資訊進行核對。
- 【0038】 D) 應用管理階段，在應用管理區中，用戶可對應用單元或應用資訊進行操作。此種操作可以是刪除、添加或修改等其他相類似的動作。
- 【0039】 如附圖2所示，對於新用戶來說，其的操作步驟爲A、B1、C1和D。如附圖3所示，對於老用戶來說，其的操作步驟爲A、B2、C2和D。

- 【0040】 如附圖1所示，一種身份認證管理裝置，它包括用戶端以及後臺。
- 【0041】 用戶端包括多個終端設備以及分別與每個終端設備相交互連接的指紋感測器，指紋感測器包括用於採集指紋資訊的採集識別裝置以及用於存儲包括指紋資訊以及該指紋資訊相對應用戶的用戶資訊的記憶體。終端設備可以是電腦、平板電腦或者手機中的一種，終端設備用於登記或識別指紋感測器採集到的指紋資訊。終端設備至少應該有一個能夠顯示操作的顯示幕，這個顯示幕能夠顯示用戶的動作。
- 【0042】 後臺包括與終端設備相交互連接的身份認證伺服器以及與身份認證伺服器相交互連接的多個應用管理區。
- 【0043】 身份認證伺服器包括用於辨別用戶身份的用户認證單元以及用於存放註冊後的用户資訊的用户檔案管理單元。
- 【0044】 應用管理區中包括應用單元以及應用資訊。應用管理區中的應用單元包括但不局限於遊戲、郵件、網站中的一種或幾種。應用管理區中的應用資訊包括但不局限於用戶名、密碼中的一種或幾種。
- 【0045】 當指紋資訊被終端設備登記或認可後，身份認證伺服器將與指紋資訊相對應的用户資訊進行生成或核對，並進入該用戶的應用管理區，在應用管理區中，可對應用單元或應用資訊進行操作。
- 【0046】 應用管理區中的應用單元還可以包括好友管理單元，好友管理單元可通過交換指紋資訊管理好友以及對於好友之間的操作。如果一位完成認證登記的用戶A在添加另一位完成登記認證的用戶B時

，掃描指紋並通過好友管理單元發送請求。B在接收到請求以及A的指紋資訊後，只要通過掃描指紋確認，並將B的指紋資訊回饋給A，就能實現好友的添加。

【0047】 應用管理區中的應用單元還包括聊天單元，用戶端上設置有用於解密或加密聊天單元中的聊天資訊的聊天軟體。

【0048】 在好友添加完成後，A與B可進行密聊。A將需要發送的資訊通過聊天軟體利用指紋資訊加密後發送給B，B在接收到資訊之後在對話方塊中顯示的是亂碼，但是B可利用指紋資訊以及聊天軟體進行解密，實現觀看。解密後，原始亂碼的文字可自動重組形成正常字體的文字，也可以是滑鼠處於亂碼文字中的任意處位置，任意處位置的亂碼文字變成正常字體或放大的文字。這樣，其他用戶即使在B的用戶端操作，但是由於他不具有B的指紋資訊，無法對聊天內容進行解密。因此，本裝置較之以往具有更好的安全性。

【0049】 終端設備與身份認證伺服器、身份認證伺服器與應用伺服器通過網路相交互連接。

【0050】 本發明採用以上結構或方法具有以下有益效果：

【0051】 1、在這個平臺上，用戶的身份是要通過指紋驗證才能夠進入應用管理區，在此基礎上就保證了用戶的私密性；

【0052】 2、用戶登記的時候，配以相對應的指紋感測器，而且相關的用戶資訊存儲在指紋感測器上，增加了用戶的安全性，減少了指紋傳感設備或者帳號遺失後對用戶資料的影響；

【0053】 3、利用指紋資訊統一管理用戶自定義的網站及其他相關應用，同時管理自定義網站以及其他應用的帳號以及密碼，使用戶能夠通過掃描指定指紋而快捷準確的登錄相關網站或者其他應用，並完成相應的帳戶登錄，節省了用戶時間的同時，也減少了在不同網站重複進行帳號登錄的麻煩，並且大大提高了安全性；

【0054】 4、具有好友添加以及好友對話功能，在未經解密的情況下，第三方無法看到私聊資訊。

【0055】 以上對本發明的特定實施例結合圖示進行了說明，很明顯，在不離開本發明的範圍和精神的基礎上，可以對現有技術和工藝進行很多修改。在本發明的所屬技術領域中，只要掌握通常知識，就可以在本發明的技術要旨範圍內，進行多種多樣的變更。

【符號說明】

【0055】

無

【發明申請專利範圍】

【第1項】 一種身份認證管理裝置，包括：

用戶端，其包括

多個終端設備，其用於登記或識別指紋感測器採集到的指紋資訊；以及

指紋感測器，分別與每個終端設備相交互連接，且包括用於採集指紋資訊的採集識別裝置以及用於存儲包括指紋資訊以及該指紋資訊相對應使用者的使用者資訊的記憶體；

後臺，其包括

身份認證伺服器，其與終端設備相交互連接；以及

多個應用管理區，其與所述身份認證伺服器相交互連接的，所述應用管理區中包括應用單元以及應用資訊；
當指紋資訊被終端設備登記或認可後，所述身份認證伺服器將與指紋資訊相對應的使用者資訊進行生成或核對，並進入該用戶的應用管理區，在應用管理區中，可對應用單元和應用資訊進行操作。

【第2項】 如申請專利範圍第1項所述的身份認證管理裝置，所述身份認證伺服器包括用於辨別用戶身份的用户認證單元以及用於存放註冊後的用户資訊的用户檔案管理單元。

【第3項】 如申請專利範圍第1項所述的身份認證管理裝置，所述終端設備與所述身份認證伺服器、所述身份認證伺服器與所述應用伺服器通過網路相交互連接。

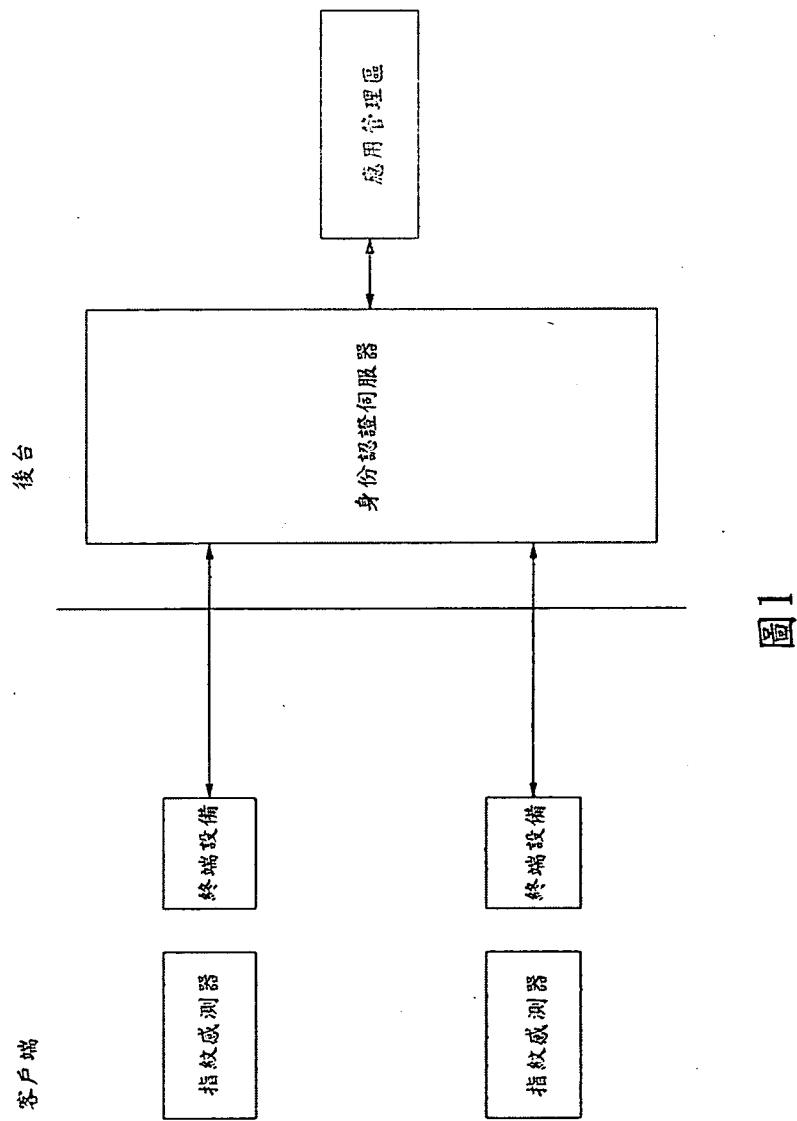
- 【第4項】 如申請專利範圍第1項所述的身份認證管理裝置，所述應用管理區中的應用單元包括但不局限於遊戲、郵件、網站中的一種或幾種。
- 【第5項】 如申請專利範圍第1項所述的身份認證管理裝置，所述應用管理區中的應用資訊包括但不局限於用戶名、密碼中的一種或幾種。
- 【第6項】 如申請專利範圍第1項所述的身份認證管理裝置，所述的應用管理區中的應用單元包括好友管理單元，該好友管理單元可通過交換指紋資訊管理好友以及對於好友之間的操作。
- 【第7項】 如申請專利範圍第1項所述的身份認證管理裝置，所述的應用管理區中的應用單元包括聊天單元，所述用戶端上設置有用於解密或加密聊天單元中的聊天資訊的聊天軟體。
- 【第8項】 一種採用如專利範圍1項所述的裝置的身份認證及管理方法，它包括以下步驟：
- A) 採集指紋資訊，通過指紋感測器的採集識別裝置提取用戶的指紋資訊；
 - B) 指紋資訊的登記或識別階段，終端設備將採集到的指紋資訊進行登記或識別；
 - C) 用戶生成或認證階段，後臺的身份認證伺服器將新登記的指紋資訊生成新的用戶資訊或將與指紋資訊相對的用戶資訊進行核對；
 - D) 應用管理階段，在應用管理區中，用戶可對應用單元或應用資訊進行操作。
- 【第9項】 如申請專利範圍第8項所述的身份認證及管理方法，該指紋感測器的採集識別裝置提取用戶的指紋資訊，終端設備將採集到的與指紋資訊相對的用戶資訊進行核對指紋資訊進行登記，後臺的身

份認證伺服器的用戶認證單元將新登記的指紋資訊生成新的用戶，並將該用戶資訊保存在身份認證伺服器的用戶檔案管理單元。

【第10項】 如申請專利範圍第8項所述的身份認證及管理方法，該指紋感測器的採集識別裝置提取用戶的指紋資訊，終端設備將採集到的指紋資訊進行識別，後臺的身份認證伺服器的用戶認證單元將存儲在用戶檔案管理單元中的用戶資訊與指紋資訊相對的用戶資訊進行核對。

【第11項】 如申請專利範圍第8項所述的身份認證及管理方法，使用者可對應用單元或應用資訊進行操作為刪除、添加或修改中的一種或幾種。

【發明圖式】



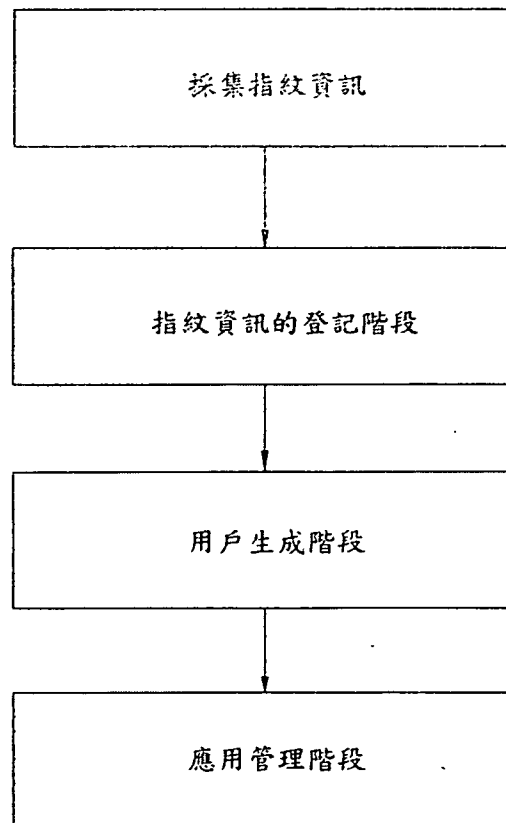


圖2

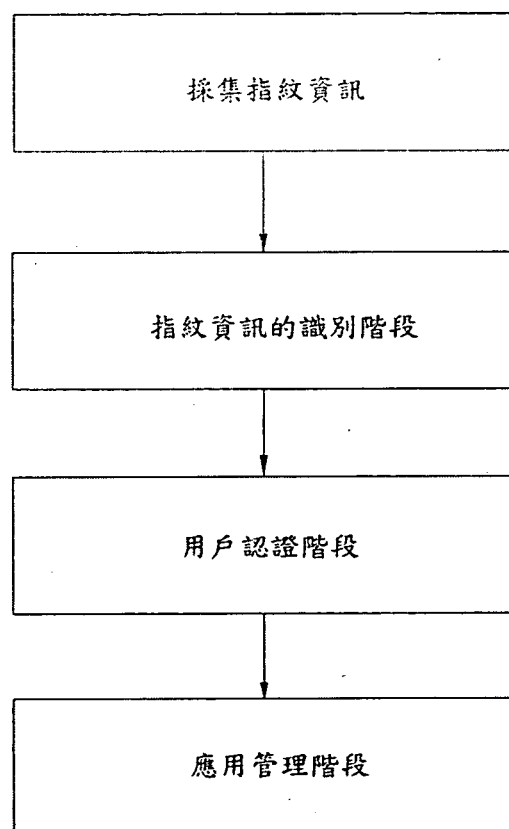


圖3