I612792

(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 I612792 B**

(45)公告日： 中華民國 107 (2018) 年 01 月 21 日

(21)申請案號：102111886 (22)申請日： 中華民國 102 (2013) 年 04 月 02 日

(51)Int. Cl.： *H04L9/32 (2006.01)* *G06K9/62 (2006.01)*

(30)優先權：2012/12/06 中國大陸 201210521715.2

(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：孟超峰 (CN) ；陳曉薇 (CN) ；陳凌雲 (CN) ；夏炎 (CN) ；許明星 (CN) ；王磊 (CN) ；祝楓 (CN) ；許吉 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	363162	TW	591459
TW	201142727A	US	20120066749A1
US	20120292388A1		

審查人員：周官緯

申請專利範圍項數：11 項 圖式數：5 共 37 頁

(54)名稱

帳戶登入的方法及裝置

(57)摘要

本發明公開了一種帳戶登入的方法及裝置，用以解決現有技術中登入帳戶的效率較低的問題。該方法終端採集用戶的第一證件的圖像，並識別採集到的圖像中包含的該用戶的用戶資訊，將識別出的用戶資訊攜帶在登入請求中發送給伺服器，以登入該用戶資訊對應的帳戶。透過上述方法，用戶在透過終端登入帳戶時，無需輸入其用戶名，直接透過終端的圖像採集設備採集第一證件的圖像，即可進行帳戶登入，有效的提高了登入帳戶的效率。

指定代表圖：

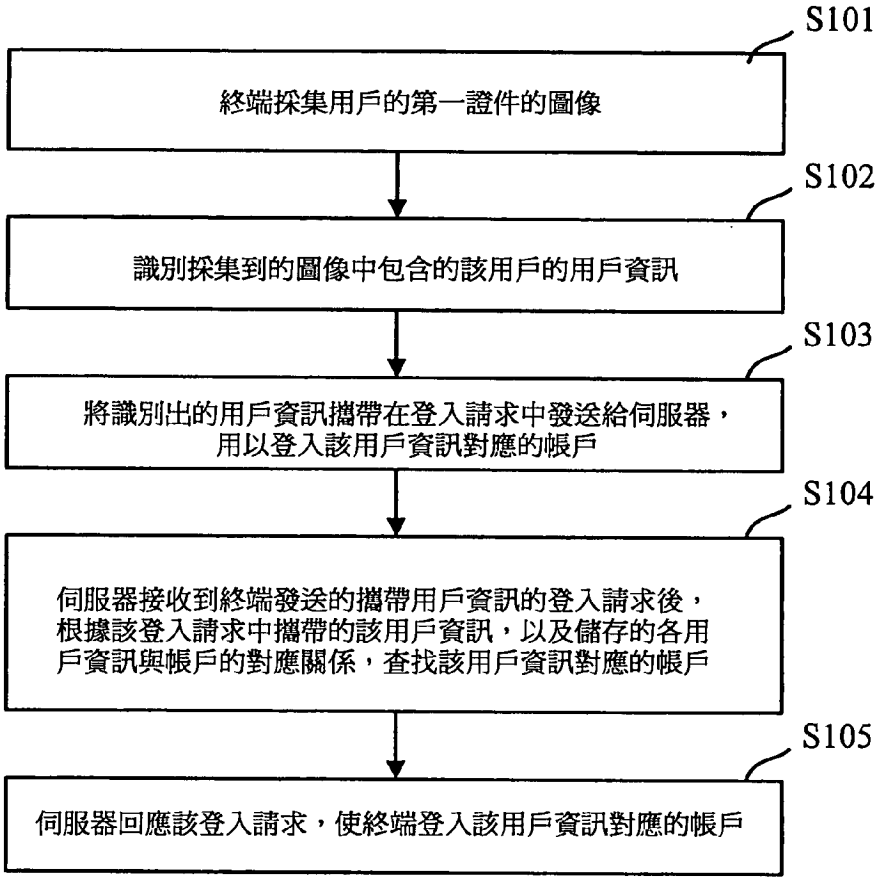
S101
終端採集用戶的第一證件的圖像
S102
識別採集到的圖像中包含的該用戶的用戶資訊
S103
將識別出的用戶資訊攜帶在登入請求中發送給伺服器，用以登入該用戶資訊對應的帳戶
S104
伺服器接收到終端發送的攜帶用戶資訊的登入請求後，根據該登入請求中攜帶的該用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找該用戶資訊對應的帳戶
S105
伺服器回應該登入請求，使終端登入該用戶資訊對應的帳戶

圖 1

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)

帳戶登入的方法及裝置

【技術領域】

本發明涉及通信技術領域，尤其涉及一種帳戶登入的方法及裝置。

【先前技術】

在現有技術中，用戶在存取網路服務時，大多要先輸入用戶名和密碼，用以登入該用戶對應於該網路服務的帳戶，然後再存取相應的網路服務。

例如，用戶在進行網路購物、或者透過即時通訊軟體與其他用戶進行通信、或者透過網路郵箱進行郵件的收發等網路服務時，均需要先輸入相應的用戶名和密碼，以登入相應的帳戶，再存取相應的網路服務。

其中，如果用戶要存取某個網路服務時，尚沒有該網路服務對應的帳戶，則可以註冊一個該網路服務對應的帳戶，在註冊帳戶時，用戶可自行設定其要註冊的帳戶所使用的用戶名和密碼，註冊成功後，則可使用該用戶名和密碼進行登入。

然而，由於目前的網路服務越來越多樣化，因此，對於一個用戶而言，該用戶就需要針對每個其所需的網路服

務註冊帳戶，也就需要該用戶牢記其註冊的每個網路服務對應的帳戶所使用的用戶名和密碼。顯然，隨著網路服務的多樣化發展，用戶是很容易忘記其註冊的帳戶所使用的用戶名和密碼的，一旦忘記，用戶就不得不透過繁瑣的步驟重新找回用戶名和密碼，這無疑降低了用戶登入帳戶的效率。

另外，目前，各種智慧行動終端已經被普遍應用，用戶除了可以透過傳統的個人電腦（Personal Computer，PC）登入帳戶以外，還可以透過諸如智慧手機、平板電腦等智慧行動終端登入帳戶。但是，由於智慧行動終端的普遍小型化，因此，用戶在透過智慧行動終端輸入用戶名和密碼時存在著諸多不便，這也進一步降低了用戶登入帳戶的效率。

【發明內容】

本發明實施例提供一種帳戶登入的方法及裝置，用以解決現有技術中登入帳戶的效率較低的問題。

本發明實施例提供的一種帳戶登入的方法，包括：

終端採集用戶的第一證件的圖像；並

識別採集到的所述圖像中包含的所述用戶的用戶資訊；以及

將識別出的所述用戶資訊攜帶在登入請求中發送給伺服器，用以登入所述用戶資訊對應的帳戶。

本發明實施例提供的一種帳戶登入的方法，包括：

伺服器接收終端發送的攜帶用戶資訊的登入請求，其中，所述登入請求中攜帶的用戶資訊是所述終端從採集到的用戶的第一證件的圖像中識別出的所述用戶的用戶資訊；並

根據所述登入請求中攜帶的所述用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找所述用戶資訊對應的帳戶；以及

回應所述登入請求，使所述終端登入所述用戶資訊對應的帳戶。

本發明實施例提供的一種帳戶登入的裝置，包括：

採集模組，用於採集用戶的第一證件的圖像；

識別模組，用於識別採集到的所述圖像中包含的所述用戶的用戶資訊；

登入模組，用於將識別出的所述用戶資訊攜帶在登入請求中發送給伺服器，用以登入所述用戶資訊對應的帳戶。

本發明實施例提供的一種帳戶登入的裝置，包括：

接收模組，用於接收終端發送的攜帶用戶資訊的登入請求，其中，所述登入請求中攜帶的用戶資訊是所述終端從採集到的用戶的第一證件的圖像中識別出的所述用戶的用戶資訊；

查找模組，用於根據所述登入請求中攜帶的所述用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找所述用戶資訊對應的帳戶；

回應模組，用於回應所述登入請求，使所述終端登入所述用戶資訊對應的帳戶。

本發明實施例提供一種帳戶登入的方法及裝置，該方法終端採集用戶的第一證件的圖像，並識別採集到的圖像中包含的該用戶的用戶資訊，將識別出的用戶資訊攜帶在登入請求中發送給伺服器，以登入該用戶資訊對應的帳戶。透過上述方法，用戶在透過終端登入帳戶時，無需輸入其用戶名，直接透過終端的圖像採集設備採集第一證件的圖像，即可進行帳戶登入，有效的提高了登入帳戶的效率。

【圖式簡單說明】

圖 1 爲本發明實施例提供的帳戶登入過程；

圖 2 爲本發明實施例提供的註冊帳戶的過程；

圖 3A 爲本發明實施例提供的終端向伺服器發送簡訊時的介面示意圖；

圖 3B 爲本發明實施例提供的終端採集圖像時的介面示意圖；

圖 3C 爲本發明實施例提供的終端採集圖像後的介面示意圖；

圖 3D 爲本發明實施例提供的終端將登入請求發送給伺服器後的介面示意圖；

圖 4 爲本發明實施例提供的一種帳戶登入的裝置結構示意圖；

圖 5 爲本發明實施例提供的另一種帳戶登入的裝置結構示意圖。

【實施方式】

本發明實施例爲了提高帳戶登入的效率，摒棄了傳統的在終端上輸入用戶名和密碼進行帳戶登入的方法，透過終端採集用戶證件的圖像，並識別採集到的圖像中包含的該用戶的用戶資訊，再基於識別出的用戶資訊登入該用戶資訊對應的帳戶。

下面結合說明書圖式對本發明實施例進行詳細描述。

圖 1 爲本發明實施例提供的帳戶登入過程，具體包括以下步驟：

S101：終端採集用戶的第一證件的圖像。

在本發明實施例中，用戶在使用終端登入帳戶時，可先透過終端採集該用戶的第一證件的圖像。其中，本發明實施例中所述的終端包括但不限於行動終端和 PC。當用戶使用 PC 登入帳戶時，可透過在 PC 的外接相機等圖像採集設備採集第一證件的圖像，當用戶使用行動終端（如手機或平板電腦等）登入帳戶時，可透過行動終端的相機等圖像採集設備採集第一證件的圖像。

具體的，該第一證件可以爲該用戶的身份證，則用戶在登入帳戶時，可透過終端採集該用戶的身份證的圖像。較佳的，當第一證件爲身份證時，終端可分別採集該用戶的身份證的正面圖像和反面圖像。

S102：識別採集到的圖像中包含的該用戶的用戶資訊。

透過上述步驟 S101 採集了第一證件的圖像後，終端則可以基於光學字元識別（Optical Character Recognition，OCR）技術來識別採集到的圖像中包含的該用戶的用戶資訊。

具體的，當上述步驟 S101 採集的第一證件的圖像是該用戶的身份證圖像時，終端可基於 OCR 技術識別採集到的圖像中包含的該用戶的姓名資訊、身份證號碼資訊中的至少一種，作爲識別出的該用戶的用戶資訊。

較佳的，當上述步驟 S101 中終端分別採集了該用戶的身份證的正面圖像和反面圖像時，終端可以從採集到的該身份證的正面圖像中識別出該用戶的姓名資訊、性別資訊、民族資訊、出生日期資訊、住址資訊、身份證號碼資訊，可以從採集到的該身份證的反面圖像中識別出該身份證的簽發機關資訊、有效期限資訊，因此，終端可將從採集到的身份證的正面圖像和反面圖像中識別出的上述資訊中的一種或幾種作爲識別出的該用戶的用戶資訊。

S103：將識別出的用戶資訊攜帶在登入請求中發送給伺服器，用以登入該用戶資訊對應的帳戶。

終端在採集到的圖像中識別出該用戶的用戶資訊後，則可將識別出的該用戶資訊攜帶在登入請求中發送給伺服器，以登入該用戶資訊對應的帳戶。

S104：伺服器接收到終端發送的攜帶用戶資訊的登入

請求後，根據該登入請求中攜帶的該用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找該用戶資訊對應的帳戶。

在本發明實施例中，伺服器中儲存了各用戶資訊與帳戶的對應關係，具體可以儲存用戶資訊與帳戶識別碼（Identity，ID）的對應關係。其中，一個用戶資訊只對應一個帳戶，一個帳戶也只對應一個用戶資訊，也即，使用一個用戶資訊只能登入一個帳戶。

S105：伺服器回應該登入請求，使終端登入該用戶資訊對應的帳戶。

伺服器查找到接收到的該登入請求中攜帶的用戶資訊對應的帳戶後，則回應該登入請求，使發送該登入請求的終端登入該用戶資訊對應的帳戶。

目前，由於相機已經成爲諸如智慧手機、平板電腦等智慧行動終端的標準配置之一，而且在 PC 上外接相機也已經非常普遍，因此，當用戶使用終端登入帳戶時，可透過上述方法，直接透過終端對該用戶自身的第一證件的圖像進行採集，終端則可以識別圖像中包含的該用戶的用戶資訊，並基於識別出的用戶資訊登入相應帳戶，從而用戶無需繁瑣的輸入用戶名，尤其是當用戶使用普遍小型化的智慧行動終端登入帳戶時，只需使用智慧行動終端採集第一證件的圖像即可，有效的提高了用戶登入帳戶的效率。

在本發明實施例中，爲了提高帳戶的安全性，在透過如圖 1 所示的方法登入帳戶時，用戶還需輸入相應的密

碼。具體的，終端在透過上述步驟 S103 將識別出的用戶資訊攜帶在登入請求中發送給伺服器之前，可提示用戶輸入密碼，在用戶輸入密碼後，則可將透過步驟 S102 識別出的用戶資訊，以及該用戶輸入的密碼攜帶在登入請求中發送給伺服器。相應的，伺服器除儲存各用戶資訊與帳戶的對應關係之外，還需儲存各帳戶所使用的密碼，當伺服器接收到攜帶用戶資訊和密碼的登入請求後，則可根據該登入請求中攜帶的用戶資訊和密碼進行驗證，在通過驗證後，再回應該登入請求，使終端登入該用戶資訊對應的帳戶。

其中，伺服器根據登入請求中攜帶的用戶資訊和密碼進行驗證的方法可以爲：伺服器確定儲存的該登入請求中攜帶的用戶資訊對應的帳戶所使用的密碼，判斷該登入請求中攜帶的密碼是否與儲存的該用戶資訊對應的密碼匹配，若匹配，則通過驗證，回應該登入請求，使終端登入該用戶資訊對應的帳戶，若不匹配，則驗證不通過，拒絕終端登入該用戶資訊對應的帳戶。

另外，在本發明實施例中，對於上述用戶資訊對應的帳戶來說，伺服器儲存該用戶資訊對應的帳戶、儲存該帳戶所使用的密碼均是在用戶註冊該帳戶時完成的，如圖 2 所示。圖 2 爲本發明實施例提供的註冊帳戶的過程，具體包括以下步驟：

S201：終端採集用戶的第一證件的圖像。

在本發明實施例中，用戶在註冊帳戶時，同樣要使用

終端對自身的第一證件的圖像進行採集，以確定其所註冊的帳戶所使用的用戶資訊。類似的，該第一證件也可以是該用戶的身份證。

S202：從採集到的圖像中識別出該用戶的用戶資訊，並提示用戶設置密碼。

類似的，終端透過 OCR 技術從採集到的圖像中識別出該用戶的用戶資訊。如果第一證件爲身份證，則可識別出圖像中的姓名資訊、身份證號碼資訊中的至少一種，作爲識別出的用戶資訊。另外，爲了保證帳戶的安全性，終端可提示用戶爲其所要註冊的帳戶設置密碼。

S203：終端將識別出的用戶資訊以及用戶設置的密碼攜帶在註冊請求中發送給伺服器。

終端在識別出用戶資訊，且用戶設置密碼完畢後，則可將識別出的用戶資訊和用戶設置的密碼攜帶在註冊請求中發送給伺服器，以註冊帳戶。

S204：伺服器接收到該註冊請求後，爲該註冊請求中攜帶的該用戶資訊分配一個帳戶。

其中，伺服器可以爲該註冊請求中攜帶的用戶資訊分配一個帳戶 ID。

S205：建立並儲存該註冊請求中攜帶的該用戶資訊與分配的該帳戶的對應關係，將該註冊請求中攜帶的改密碼作爲分配的該帳戶所使用的密碼儲存。

此時，本次帳戶註冊已經成功，後續的，當用戶要登入該帳戶時，則可以透過如圖 1 所示的方法，使用終端採

集該第一證件（註冊該帳戶時所使用的第一證件）的圖像，並輸入密碼，即可登入該帳戶。

進一步的，爲了進一步提高帳戶的安全性，在透過如圖 2 所示的過程進行帳戶註冊時，上述步驟 S203 中，終端還可以將該終端的終端標識也攜帶在註冊請求中發送給伺服器，此時，步驟 S205 中，伺服器接收到該註冊請求後，除建立該註冊請求中攜帶的該用戶資訊與分配的帳戶的對應關係以外，還要建立該註冊請求中攜帶的該終端標識與分配的該帳戶的對應關係。

相應的，在透過如圖 1 所示的過程進行帳戶登入時，終端也要將用戶資訊（從採集的第一證件的圖像中識別出的用戶資訊）、用戶輸入的密碼以及終端自身的終端標識攜帶在登入請求中發送給伺服器，伺服器接收到該登入請求後，則可以查找該登入請求中攜帶的用戶資訊對應的帳戶，並判斷儲存的該帳戶對應的終端標識是否爲該登入請求中攜帶的終端標識，以及該帳戶所使用的密碼是否與登入請求中攜帶的密碼匹配，若均爲是，則通過驗證，回應該登入請求，使終端登入該用戶資訊對應的帳戶，若至少一個爲否，則驗證不通過，拒絕終端登入該用戶資訊對應的帳戶。

當然，伺服器在查找該登入請求中攜帶的用戶資訊對應的帳戶後，驗證該登入請求中攜帶的密碼與儲存的該帳戶所使用的密碼相同，但該登入請求中攜帶的終端標識與該帳戶對應的終端標識不同時，也可以判定爲通過驗證，

允許終端登入帳戶，此時，伺服器可以更新儲存的該帳戶對應的終端標識，即，將儲存的該帳戶對應的終端標識更新爲該登入請求中攜帶的終端標識。

當然，終端也可以先將自身的終端標識發送給伺服器，則伺服器查找該終端標識對應的帳戶，然後終端再將用戶資訊和用戶輸入的密碼攜帶在登入請求中發送給伺服器，伺服器則驗證登入請求中攜帶的用戶資訊是否爲查找到的帳戶對應的用戶資訊，驗證登入請求中攜帶的密碼是否爲查找到的帳戶所使用的密碼，若驗證均通過，則允許終端登入，否則拒絕登入。

其中，當上述終端是智慧行動終端時，該終端的終端標識包括但不限於該終端的手機號和國際行動用戶識別碼（International Mobile Subscriber Identification，IMSI）號。當終端標識爲手機號時，終端向伺服器發送自身的終端標識的方法可以爲向該伺服器發送簡訊，此時，在終端登入帳戶的過程中，終端的介面可分別如圖 3A~圖 3D 所示。

圖 3A 爲本發明實施例提供的終端向伺服器發送簡訊時的介面示意圖，如圖 3A 所示，在用戶透過終端登入帳戶的過程中，終端的介面以進度條的形式來提示用戶登入過程中所需的步驟，並可以以文字的形式添加當前所進行的步驟的備註資訊。由於在圖 3A 所示的登入帳戶過程中，終端需要向伺服器發送簡訊，因此，圖 3A 所示的介面中設置了一個“發送簡訊”的按鈕，透過點擊該按鈕，

即可使終端向伺服器發送簡訊。伺服器接收到該簡訊後，即可得到該終端的終端標識，也即手機號碼。

圖 3B 爲本發明實施例提供的終端採集圖像時的介面示意圖，如圖 3B 所示，該介面中設置了一個“掃描”按鈕，透過點擊該按鈕，即可開始採集第一證件的圖像。

圖 3C 爲本發明實施例提供的終端採集圖像後的介面示意圖，如圖 3C 所示，該介面中顯示了從採集的第一證件的圖像中識別出的用戶資訊，用以提供給用戶進行確認，若用戶確認識別出的用戶資訊無誤，則可以點擊該介面中的“確認資訊”按鈕，則該用戶資訊將被攜帶在登入請求中發送給伺服器，若用戶發現識別出的用戶資訊錯誤，則可點擊介面中的“重新採集”按鈕，以重新採集第一證件的圖像，並重新進行用戶資訊的識別。

圖 3D 爲本發明實施例提供的終端將登入請求發送給伺服器後的介面示意圖，如圖 3D 所示，終端將攜帶用戶資訊的登入請求發送給伺服器後，伺服器已經通過驗證，該介面上設置了一個“開始使用”按鈕，透過點擊該按鈕，則可見該介面切換到帳戶介面，以存取相應的網路服務。

更進一步的，爲了提高帳戶的安全性，本發明實施例在透過如圖 2 所示的方法註冊帳戶時，除了將從採集的第一證件的圖像中識別出的用戶資訊以及用戶設置的密碼攜帶在註冊請求中發送給伺服器以外，還可將採集的該第一證件的圖像也攜帶在註冊請求中發送給伺服器，伺服器則

建立分配的帳戶與註冊請求中攜帶的用戶資訊的對應關係，建立分配的帳戶與註冊請求中攜帶的圖像的對應關係，並將註冊請求中攜帶的密碼儲存爲該分配的帳戶所使用的密碼。

相應的，在透過如圖 1 所示的方法登入帳戶時，終端採集了第一證件的圖像後，除了要將從採集的第一證件的圖像中識別出的用戶資訊以及用戶輸入的密碼攜帶在登入請求中發送給伺服器以外，還要將採集的第一證件的圖像也攜帶在登入請求中發送給伺服器。伺服器接收到登入請求後，則可查找登入請求中攜帶的用戶資訊對應的帳戶，並判斷該登入請求中攜帶的密碼是否與儲存的該帳戶對應的密碼匹配，判斷該登入請求中攜帶的圖像與儲存的該帳戶對應的圖像的相似度是否大於設定閾值，若判斷結果均爲是，則通過驗證，回應該登入請求，使該終端登入該用戶資訊對應的帳戶，否則，驗證不通過，拒絕終端登入帳戶。

另外，爲了盡可能的保護用戶的隱私，在透過如圖 2 所示的過程註冊帳戶時，伺服器儲存用戶資訊和密碼的方法可以爲：將接收到的註冊請求中攜帶的用戶資訊和密碼進行加密，得到加密後的用戶資訊和加密後的密碼，再建立並儲存分配的帳戶與加密後的用戶資訊的對應關係，將加密後的密碼作爲分配的帳戶所使用的密碼儲存。

其中，對用戶資訊和密碼進行加密時，可基於不可逆的加密演算法進行加密，也即採用不可解密的加密演算法

對用戶資訊和密碼進行加密，得到加密後的用戶資訊和加密後的密碼。以下將未加密的用戶資訊稱爲明文用戶資訊，將未加密的用戶資訊稱爲明文密碼，將加密後的用戶資訊稱爲密文用戶資訊，將加密後的密碼稱爲密文密碼。

如果伺服器在儲存用戶資訊和密碼時不對其進行加密，則伺服器中就會儲存用戶註冊帳戶時所使用的明文用戶資訊和明文密碼，這樣，一旦伺服器遭到惡意攻擊，用戶資訊和密碼就極易被洩露，嚴重影響了用戶隱私的安全性。但是，採用不可逆的加密演算法進行加密後，伺服器中儲存的是密文用戶資訊和密文密碼，因此，即使伺服器遭到惡意攻擊而洩露出密文用戶資訊和密文密碼，該密文用戶資訊和密文密碼也是不可直接被人爲解讀的，也不可被解密，從而可以有效的保護用戶隱私。

相應的，當伺服器中儲存了密文用戶資訊和密文密碼時，採用如圖 1 所示的方法登入帳戶時，伺服器接收到攜帶明文用戶資訊和明文密碼的登入請求後，則可以採用同樣的不可逆的加密演算法（與註冊帳戶時採用的加密演算法相同），對登入請求中攜帶的明文用戶資訊和明文密碼進行加密，得到密文用戶資訊和密文密碼，然後，伺服器再查找該密文用戶資訊對應的帳戶，並驗證得到的密文密碼是否與儲存的該帳戶所使用的密文密碼匹配，若驗證通過，則允許終端登入該帳戶。

在本發明實施例中，爲了進一步提高帳戶的安全性，還可以根據實際需要預先設定一些指定操作，終端在用戶

進行這些指定操作時，則採集該用戶的第二證件的圖像，並識別採集到的第二證件的圖像中包含的校驗資訊，再將透過第一證件的圖像識別出的用戶資訊以及透過第二證件的圖像識別出的校驗資訊攜帶在與該指定操作對應的請求訊息中發送給伺服器，伺服器接收到該請求訊息後，則根據該請求訊息中攜帶的用戶資訊以及校驗資訊進行驗證，並在通過驗證後，回應該請求訊息，使終端執行該指定操作的相關步驟。

其中，上述指定操作可以設置爲重置密碼操作，也可以設置爲其他種類的操作。如，當用戶登入帳戶後，頻繁向伺服器請求同一個操作時，則可將用戶頻繁請求的該操作作爲指定操作；或者，在透過圖 1 所示的方法登入帳戶時，如果用戶本次登入帳戶所使用的終端不同於上一次登入該帳戶所使用的終端，或者，如果用戶當前的帳戶安全級別較低，則可將本次用戶登入該帳戶的操作作爲指定操作。

下面以該指定操作爲重置密碼操作爲例進行說明。

考慮到當用戶透過爲其註冊的帳戶設置了密碼時，很有可能會忘記其設置的密碼，而現有技術中找回並重置密碼的方法通常是透過簡訊校驗、郵箱找回、密碼提示問題等方法，其重置密碼的步驟較爲繁瑣，效率較爲低下。

因此，基於與上述帳戶登入和帳戶註冊類似的思路，爲了提高重置密碼的效率，本發明實施例提供了一種重置密碼的方法，具體包括：終端在用戶進行重置密碼操作

時，採集用戶的第二證件的圖像，並識別採集到的該第二證件的圖像中包含的校驗資訊，將透過第一證件的圖像識別出的用戶資訊以及透過第二證件的圖像識別出的校驗資訊攜帶在密碼重置請求（即與密碼重置操作對應的請求訊息）中發送給伺服器，在伺服器根據該密碼重置請求中攜帶的用戶資訊和校驗資訊進行通過驗證後，執行重置密碼的相關步驟。

其中，用戶可以在透過如圖 1 所示的方法成功登入了帳戶之後，進行重置密碼操作，也可以是在忘記密碼時，透過如圖 1 所示的方法未成功登入帳戶後，進行重置密碼的操作。當用戶忘記密碼時，透過如圖 1 所示的方法使用終端採集了第一證件的圖像，但輸入了錯誤的密碼，則終端將從第一證件的圖像中識別出的用戶資訊和錯誤的密碼攜帶在登入請求中發送給伺服器後，伺服器會拒絕終端登入帳戶，此時，用戶可發起重置密碼操作，由於終端已經採集到了第一證件的圖像，並從中識別出了用戶資訊，因此，用戶發起重置密碼後，可提示用戶使用終端採集第二證件的圖像，並從第二證件的圖像中識別出校驗資訊，再將用戶資訊和校驗資訊攜帶在密碼重置請求中發送給伺服器，當伺服器根據該用戶資訊和校驗資訊通過驗證後，則可執行後續重置密碼的相關步驟。

進一步的，上述第二證件可以是該用戶的銀行卡，也即當用戶進行重置密碼操作時，終端採集該用戶的銀行卡的圖像，並識別採集的該銀行卡的圖像中包含的銀行卡卡

S

號資訊，作爲校驗資訊。此時，終端則可將用戶資訊（用戶的姓名資訊、身份證號碼資訊）和校驗資訊（銀行卡卡號資訊）攜帶在密碼重置請求中發送給伺服器。

伺服器接收到該密碼重置請求後，根據該密碼重置請求中攜帶的用戶資訊和校驗資訊進行驗證的方法具體可以爲：透過與銀行系統進行通信，以驗證作爲校驗資訊的銀行卡卡號所對應的用戶姓名是否與密碼重置請求中攜帶的姓名相同，驗證該銀行卡卡號所對應的身份證號碼是否與密碼重置請求中攜帶的身份證號碼相同，若均相同，則通過驗證，回應該密碼重置請求，使該終端執行後續重置密碼的相關步驟，否則，驗證不通過，拒絕該密碼重置請求。

當然，也可以在上述驗證方法的基礎上，採用其他附件方法對密碼重置請求中攜帶的用戶資訊和校驗資訊進行進一步的驗證。

例如，當用戶使用的終端是智慧手機時，如果伺服器透過銀行系統已經驗證了作爲校驗資訊的銀行卡卡號所對應的用戶姓名是密碼重置請求中攜帶的姓名，該銀行卡卡號所對應的身份證號碼也是密碼重置請求中攜帶的身份證號碼，則還可透過與銀行系統的通信，進一步指示銀行系統向該密碼重置請求中攜帶的銀行卡卡號對應的預留手機號碼發送驗證簡訊，該驗證簡訊中攜帶驗證碼，並向終端（智慧手機）發送存取驗證碼的請求。終端則提示用戶輸入驗證碼，並將用戶輸入的驗證碼發送給伺服器，伺服器

再將接收到的驗證碼發送給銀行系統，銀行系統對比發送的驗證簡訊中攜帶的驗證碼以及伺服器發來的驗證碼，並向伺服器返回對比結果。如果伺服器接收到的對比結果是二者相同，則說明用戶當前使用的終端（智慧手機）的手機號碼是該銀行卡卡號所對應的預留手機號碼，因此通過驗證，否則說明用戶當前使用的終端（智慧手機）的手機號碼不是該銀行卡卡號所對應的預留手機號碼，因此驗證不通過。

上述只是以第一證件爲身份證，第二證件爲銀行卡爲例對本發明實施例提供的帳戶登入方法進行說明的，基於本發明實施例提供的上述帳戶登入方法，身份證、銀行卡、護照、駕照等證件均可作爲第一證件或第二證件應用到上述方法中，可達到同樣的效果。

另外，由於本發明實施例主要是透過終端採集圖像來登入帳戶的，因此，基於同樣的思路，用戶在註冊帳戶時，也可以使用終端採集其他圖像進行註冊，例如採集自己的名片的圖像，甚至某一處風景的圖像，伺服器建立終端發來的圖像（攜帶在註冊請求中）與分配的帳戶的對應關係，後續終端登入帳戶時，只要能夠採集到註冊該帳戶時所採集的圖像，即可登入到相應的帳戶。

以上是本發明實施例提供的帳戶登入的方法，基於同樣的思路，本發明還提供一種帳戶登入的裝置，如圖 4 和圖 5 所示。

圖 4 爲本發明實施例提供的一種帳戶登入的裝置結構

S

示意圖，具體包括：

採集模組 401，用於採集用戶的第一證件的圖像；

識別模組 402，用於識別採集到的所述圖像中包含的所述用戶的用戶資訊；

登入模組 403，用於將識別出的所述用戶資訊攜帶在登入請求中發送給伺服器，用以登入所述用戶資訊對應的帳戶。

所述採集模組 401 具體用於，採集所述用戶的身份證的圖像；

所述識別模組 402 具體用於，識別採集到的所述圖像中包含的所述用戶的姓名資訊、身份證號碼資訊中的至少一種。

所述登入模組 403 具體用於，將識別出的所述用戶資訊，以及所述用戶輸入的密碼攜帶在登入請求中發送給伺服器，並在所述伺服器根據所述登入請求中攜帶的所述用戶資訊和密碼進行通過驗證後，登入所述用戶資訊對應的帳戶，其中，所述伺服器中儲存了用戶資訊與帳戶的對應關係，以及各帳戶所使用的密碼。

所述採集模組 401 還用於，在所述用戶進行指定操作時，採集所述用戶的第二證件的圖像，其中，所述指定操作包括重置密碼操作；

所述識別模組 402 還用於，識別採集到的所述第二證件的圖像中包含的校驗資訊；

所述裝置還包括：

指定操作模組 404，用於將透過所述第一證件的圖像識別出的用戶資訊以及透過所述第二證件的圖像識別出的校驗資訊攜帶在與所述指定操作對應的請求訊息中發送給伺服器，在所述伺服器根據所述請求訊息中攜帶的所述用戶資訊和所述校驗資訊進行通過驗證後，執行所述指定操作的相關步驟。

所述採集模組 401 具體用於，採集所述用戶的銀行卡的圖像；

所述識別模組 402 具體用於，識別採集到的所述第二證件的圖像中包含的銀行卡卡號資訊。

具體的上述圖 4 所示的帳戶登入的裝置可以位於終端中。

圖 5 爲本發明實施例提供的另一種帳戶登入的裝置結構示意圖，具體包括：

接收模組 501，用於接收終端發送的攜帶用戶資訊的登入請求，其中，所述登入請求中攜帶的用戶資訊是所述終端從採集到的用戶的第一證件的圖像中識別出的所述用戶的用戶資訊；

查找模組 502，用於根據所述登入請求中攜帶的所述用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找所述用戶資訊對應的帳戶；

回應模組 503，用於回應所述登入請求，使所述終端登入所述用戶資訊對應的帳戶。

所述接收模組 501 具體用於，接收所述終端發送的攜

帶用戶資訊以及密碼的登入請求，其中，所述密碼是用戶透過所述終端輸入的；

所述回應模組 503 還用於，在回應所述登入請求之前，確定儲存的所述用戶資訊對應的帳戶所使用的密碼，並確定所述登入請求中攜帶的密碼與儲存的所述用戶資訊對應的帳戶所使用的密碼匹配。

所述接收模組 501 還用於，接收終端發送的攜帶用戶資訊以及密碼的註冊請求，其中，所述註冊請求中攜帶的用戶資訊是所述終端從採集到的用戶的第一證件的圖像中識別出的所述用戶的用戶資訊，所述註冊資訊中攜帶的密碼是所述用戶透過所述終端設置的密碼；

所述裝置還包括：

管理模組 504，用於爲所述註冊請求中攜帶的所述用戶資訊分配一個帳戶，建立並儲存所述註冊請求中攜帶的所述用戶資訊與分配的所述帳戶的對應關係，將所述註冊請求中攜帶的所述密碼作爲分配的所述帳戶所使用的密碼儲存。

所述接收模組 501 還用於，接收所述終端發送的攜帶所述用戶資訊以及校驗資訊的、且與指定操作對應的請求訊息，其中，所述請求訊息中攜帶的所述校驗資訊是所述終端從採集到的用戶的第二證件的圖像中識別出的校驗資訊，所述指定操作包括重置密碼操作；

所述回應模組 503 還用於，當所述接收模組 501 接收到所述終端發送的請求訊息時，根據所述用戶資訊以及所

述校驗資訊進行驗證，並在通過驗證後，回應所述請求訊息，使所述終端執行所述指定操作的相關步驟。

具體的上述如圖 5 所示的帳戶登入的裝置可以位於伺服器中。

本發明實施例提供一種帳戶登入的方法及裝置，該方法終端採集用戶的第一證件的圖像，並識別採集到的圖像中包含的該用戶的用戶資訊，將識別出的用戶資訊攜帶在登入請求中發送給伺服器，以登入該用戶資訊對應的帳戶。透過上述方法，用戶在透過終端登入帳戶時，無需輸入其用戶名，直接透過終端的圖像採集設備採集第一證件的圖像，即可進行帳戶登入，有效的提高了登入帳戶的效率。

本領域內的技術人員應明白，本發明的實施例可提供爲方法、系統、或電腦程式產品。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電腦可用程式碼的電腦可用儲存介質（包括但不限於磁盤記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

本發明是參照根據本發明實施例的方法、設備（系統）、和電腦程式產品的流程圖和／或圖來描述的。應理解可由電腦程式指令實現流程圖和／或圖中的每一流程和／或、以及流程圖和／或圖中的流程和／或的結合。可提供這些電腦程式指令到通用電腦、專用電腦、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，使得透過電腦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／或圖一個或多個中指定的功能的裝置。

這些電腦程式指令也可儲存在能引導電腦或其他可編程資料處理設備以特定方式工作的電腦可讀記憶體中，使得儲存在該電腦可讀記憶體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／或圖一個或多個中指定的功能。

這些電腦程式指令也可裝載到電腦或其他可編程資料處理設備上，使得在電腦或其他可編程設備上執行一系列操作步驟以產生電腦實現的處理，從而在電腦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／或圖一個或多個中指定的功能的步驟。

儘管已描述了本發明的優選實施例，但本領域內的技術人員一旦得知了基本創造性概念，則可對這些實施例做出另外的變更和修改。所以，所附申請專利範圍意欲解釋爲包括優選實施例以及落入本發明範圍的所有變更和修改。

顯然，本領域的技術人員可以對本發明進行各種改動和變型而不脫離本發明的精神和範圍。這樣，倘若本發明的這些修改和變型屬於本發明申請專利範圍及其等同技術的範圍之內，則本發明也意圖包含這些改動和變型在內。

【符號說明】

401：採集模組

402：識別模組

403：登入模組

404：指定操作模組

501：接收模組

502：查找模組

503：回應模組

504：管理模組

公告本

發明摘要

※申請案號：102111886

※申請日：102 年 04 月 02 日　　※IPC 分類：*H04L 9/32* (2006.01)
G06K 9/62 (2006.01)

【發明名稱】(中文/英文)

帳戶登入的方法及裝置

【中文】

本發明公開了一種帳戶登入的方法及裝置，用以解決現有技術中登入帳戶的效率較低的問題。該方法終端採集用戶的第一證件的圖像，並識別採集到的圖像中包含的該用戶的用戶資訊，將識別出的用戶資訊攜帶在登入請求中發送給伺服器，以登入該用戶資訊對應的帳戶。透過上述方法，用戶在透過終端登入帳戶時，無需輸入其用戶名，直接透過終端的圖像採集設備採集第一證件的圖像，即可進行帳戶登入，有效的提高了登入帳戶的效率。

【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

第 102111886 號　　民國 106 年 2 月 15 日修正

申請專利範圍

1.一種帳戶登入的方法，其特徵在於，包括：

行動終端採集用戶的第一證件的圖像；並

識別採集到的該圖像中包含的該用戶的用戶資訊；以及

將識別出的該用戶資訊攜帶在登入請求中發送給伺服器，用以登入該用戶資訊對應的帳戶。

2.如申請專利範圍第 1 項所述的方法，其中，採集該用戶的第一證件的圖像，具體包括：

採集該用戶的身份證的圖像；

識別採集到的該圖像中包含的該用戶的用戶資訊，具體包括：

識別採集到的該圖像中包含的該用戶的姓名資訊、身份證號碼資訊中的至少一種。

3.如申請專利範圍第 1 項所述的方法，其中，將識別出的該用戶資訊攜帶在登入請求中發送給伺服器，具體包括：

將識別出的該用戶資訊，以及該用戶輸入的密碼攜帶在登入請求中發送給伺服器；

登入該用戶資訊對應的帳戶，具體包括：

在該伺服器根據該登入請求中攜帶的該用戶資訊和密碼進行通過驗證後，登入該用戶資訊對應的帳戶，其中，該伺服器中儲存了用戶資訊與帳戶的對應關係，以及各帳戶所使用的密碼。

4.如申請專利範圍第 3 項所述的方法，其中，該方法還包括：

該行動終端在該用戶進行指定操作時，採集該用戶的第二證件的圖像，其中，該指定操作包括重置密碼操作；並

識別採集到的該第二證件的圖像中包含的校驗資訊；以及

將透過該第一證件的圖像識別出的用戶資訊以及透過該第二證件的圖像識別出的校驗資訊攜帶在與該指定操作對應的請求訊息中發送給伺服器；

在該伺服器根據該請求訊息中攜帶的該用戶資訊和該校驗資訊進行通過驗證後，執行該指定操作的相關步驟。

5.如申請專利範圍第 4 項所述的方法，其中，採集該用戶的第二證件的圖像，具體包括：

採集該用戶的銀行卡的圖像；

識別採集到的該第二證件的圖像中包含的校驗資訊，具體包括：

識別採集到的該第二證件的圖像中包含的銀行卡卡號資訊。

6.一種帳戶登入的方法，其特徵在於，包括：

伺服器接收行動終端發送的攜帶用戶資訊的登入請求，其中，該登入請求中攜帶的用戶資訊是該行動終端從採集到的用戶的第一證件的圖像中識別出的該用戶的用戶資訊；並

根據該登入請求中攜帶的該用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找該用戶資訊對應的帳戶；以及

回應該登入請求，使該行動終端登入該用戶資訊對應的帳戶。

7.如申請專利範圍第 6 項所述的方法，其中，伺服器接收行動終端發送的攜帶用戶資訊的登入請求，具體包括：

該伺服器接收該行動終端發送的攜帶用戶資訊以及密碼的登入請求，其中，該密碼是用戶透過該行動終端輸入的；

回應該登入請求之前，該方法還包括：

該伺服器確定儲存的該用戶資訊對應的帳戶所使用的密碼，並確定該登入請求中攜帶的密碼與儲存的該用戶資訊對應的帳戶所使用的密碼匹配。

8.如申請專利範圍第 7 項所述的方法，其中，該伺服器儲存該用戶資訊與相應帳戶的對應關係，並儲存該用戶資訊對應的帳戶所使用的密碼，具體包括：

該伺服器接收行動終端發送的攜帶用戶資訊以及密碼的註冊請求，其中，該註冊請求中攜帶的用戶資訊是該行動終端從採集到的用戶的第一證件的圖像中識別出的該用戶的用戶資訊，該註冊請求中攜帶的密碼是該用戶透過該行動終端設置的密碼；並

爲該註冊請求中攜帶的該用戶資訊分配一個帳戶，建

立並儲存該註冊請求中攜帶的該用戶資訊與分配的該帳戶的對應關係，將該註冊請求中攜帶的該密碼作爲分配的該帳戶所使用的密碼儲存。

9.一種帳戶登入的裝置，其特徵在於，包括：

接收模組，用於接收行動終端發送的攜帶用戶資訊的登入請求，其中，該登入請求中攜帶的用戶資訊是該行動終端從採集到的用戶的第一證件的圖像中識別出的該用戶的用戶資訊；

查找模組，用於根據該登入請求中攜帶的該用戶資訊，以及儲存的各用戶資訊與帳戶的對應關係，查找該用戶資訊對應的帳戶；

回應模組，用於回應該登入請求，使該行動終端登入該用戶資訊對應的帳戶。

10.如申請專利範圍第 9 項所述的裝置，其中，該接收模組具體用於，接收該行動終端發送的攜帶用戶資訊以及密碼的登入請求，其中，該密碼是用戶透過該行動終端輸入的；

該回應模組還用於，在回應該登入請求之前，確定儲存的該用戶資訊對應的帳戶所使用的密碼，並確定該登入請求中攜帶的密碼與儲存的該用戶資訊對應的帳戶所使用的密碼匹配。

11.如申請專利範圍第 10 項所述的裝置，其中，該接收模組還用於，接收行動終端發送的攜帶用戶資訊以及密碼的註冊請求，其中，該註冊請求中攜帶的用戶資訊是該

行動終端從採集到的用戶的第一證件的圖像中識別出的該用戶的用戶資訊，該註冊資訊中攜帶的密碼是該用戶透過該行動終端設置的密碼；

該裝置還包括：

管理模組，用於爲該註冊請求中攜帶的該用戶資訊分配一個帳戶，建立並儲存該註冊請求中攜帶的該用戶資訊與分配的該帳戶的對應關係，將該註冊請求中攜帶的該密碼作爲分配的該帳戶所使用的密碼儲存。