I632484

(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 I632484 B**

(45)公告日： 中華民國 107 (2018) 年 08 月 11 日

(21)申請案號：103134017 (22)申請日： 中華民國 103 (2014) 年 09 月 30 日

(51)Int. Cl.： *G06F21/60 (2013.01)* *G06Q30/06 (2012.01)*

(30)優先權：2014/06/12 中國大陸 201410262185.3

(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：李立中 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	201122854A	TW	201218106A
US	2006/0200855A1	US	2010/0295679A1
US	2013/0111208A1	US	2013/0191640A1
US	2014/0115708A1		

審查人員：李國隆

申請專利範圍項數：12 項 圖式數：10 共 45 頁

(54)名稱

資訊保密方法及相關裝置

(57)摘要

本申請實施例公開了一種資訊保密方法及相關裝置，通過伺服器設置與目標資訊保密部分對應的識別字，儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；移動終端獲取並向伺服器發送本身的所在地資訊和待識別的識別字；伺服器判斷所述所在地資訊與所述第一位址資訊是否一致，如果一致，則將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。應用本申請，只有當移動終端的所在地資訊與第一位址資訊相同，即送貨人員到達第一位址資訊對應的位址範圍內時，移動終端才可以得到完整的目標資訊，因此，本申請可以實現對目標資訊的保密。

指定代表圖：

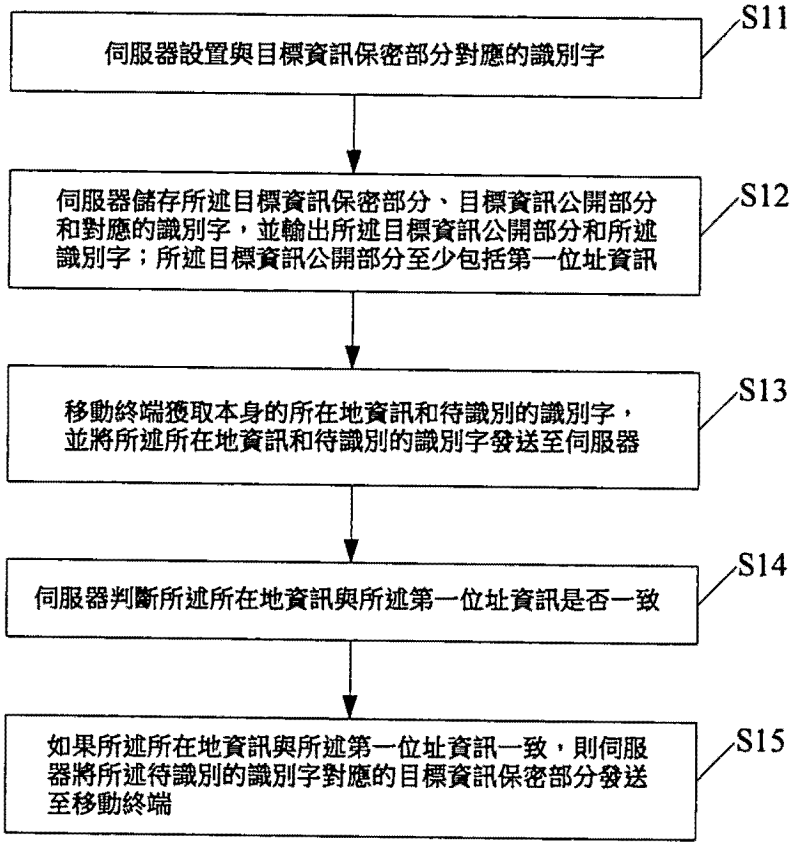
伺服器設置與目標資訊保密部分對應的識別字
S11
伺服器儲存所述目標資訊保密部分、目標資訊公開部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊
S12
移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器
S13
伺服器判斷所述所在地資訊與所述第一位址資訊是否一致
S14
如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端
S15

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)

資訊保密方法及相關裝置

【技術領域】

[0001] 本發明關於通信技術領域，特別是關於一種資訊保密方法及相關裝置。

【先前技術】

[0002] 隨著網路技術的快速發展，網路購物越來越普遍。買家在下單付款的同時，將收貨位址、聯繫電話等個人資訊提供給賣家，賣家將商品通過物流公司寄送至買家提供的收貨地址。

[0003] 在上述交易過程中，甚至交易完成後，買家的個人資訊都是完全公開的，極易通過明示有這些資訊的快遞詳情單等洩露，對買家隱私構成威脅，例如給買家撥打騷擾電話、寄送特殊物品等。因此，如何在不影響正常交易的前提下，實現對買家個人資訊的保密已成為一個亟待解決的問題。

【發明內容】

[0004] 本申請實施例中提供了一種資訊保密方法及相關裝置，以解決網路購物過程中買家個人資訊易被洩露

的問題。

[0005] 為了解決上述技術問題，本申請實施例公開了如下技術方案：

[0006] 第一方面，提供一種資訊保密方法；所述資訊保密方法包括：

[0007] 伺服器設置與目標資訊保密部分對應的識別字；

[0008] 伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；

[0009] 移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器；

[0010] 伺服器判斷所述所在地資訊與所述第一位址資訊是否一致；

[0011] 如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0012] 結合第一方面，在第一方面第一種可能的實現方式中，所述資訊保密方法還包括：在將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器刪除本身儲存的與所述待識別的識別字對應的目標資訊保密部分。

[0013] 結合第一方面，或者第一方面第一種可能的實現方式，在第一方面第二種可能的實現方式中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0014] 結合第一方面，或者第一方面第一種可能的實現方式，在第一方面第三種可能的實現方式中，所述目標資訊保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0015] 結合第一方面，或者第一方面第一種可能的實現方式，在第一方面第四種可能的實現方式中，所述伺服器設置與目標資訊保密部分對應的識別字，包括：伺服器根據預設加密規則對所述目標資訊保密部分進行加密處理，得到所述識別字。

[0016] 第二方面，提供一種資訊保密方法；所述資訊保密方法包括：

[0017] 伺服器設置與目標資訊保密部分對應的識別字；

[0018] 伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；

[0019] 伺服器接收移動終端發送的所在地資訊和待識別的識別字；

[0020] 伺服器判斷所述所在地資訊與所述第一位址資訊是否一致；

[0021] 如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0022] 結合第二方面，在第二方面第一種可能的實現方式中，所述資訊保密方法還包括：在將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器刪除本身儲存的與所述待識別的識別字對應的目標資訊保密部分。

[0023] 結合第二方面，或者第二方面第一種可能的實現方式，在第二方面第二種可能的實現方式中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0024] 結合第二方面，或者第二方面第一種可能的實現方式，在第二方面第三種可能的實現方式中，所述目標資訊保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0025] 結合第二方面，或者第二方面第一種可能的實現方式，在第二方面第四種可能的實現方式中，所述伺服器設置與目標資訊保密部分對應的識別字，包括：伺服器根據預設加密規則對所述目標資訊保密部分進行加密處理，得到所述識別字。

[0026] 協力廠商面，提供一種資訊保密方法；所述資訊保密方法包括：

[0027] 移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器；

[0028] 移動終端接收伺服器按照以下方式回饋的目標資訊保密部分：伺服器判斷所述所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果所述所在地資訊與所述第一位址資訊一致，則伺服器將待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0029] 結合協力廠商面，在協力廠商面第一種可能的實現方式中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0030] 結合協力廠商面，在協力廠商面第二種可能的實現方式中，所述目標資訊保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0031] 第四方面，提供一種伺服器；所述伺服器包括：

[0032] 設置單元，用於設置與目標資訊保密部分對應的識別字；

[0033] 儲存單元，用於儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字；所述目標資訊公開部分至少包括第一位址資訊；

[0034] 輸出單元，用於輸出所述目標資訊公開部分和所述識別字；

[0035] 接收單元，用於接收移動終端發送的所在地資訊和待識別的識別字；

[0036] 判斷單元，用於判斷所述所在地資訊與所述第一位址資訊是否一致；

[0037] 發送單元，用於在所述所在地資訊與所述第一位址資訊一致時，將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0038] 結合第四方面，在第四方面第一種可能的實現方式中，所述伺服器還包括：更新單元，用於在將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，刪除所述儲存單元中與所述待識別的識別字對應的目標資訊保密部分。

[0039] 第五方面，提供一種移動終端；所述移動終端包括：

[0040] 獲取單元，用於獲取移動終端的所在地資訊和待識別的識別字；

[0041] 發送單元，用於將所述所在地資訊和待識別的識別字發送至伺服器；

[0042] 接收單元，用於接收伺服器按照以下方式回饋的目標資訊保密部分：伺服器判斷所述所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識

別的識別字對應的目標資訊保密部分發送至移動終端。

[0043] 由以上技術方案可見，本申請通過伺服器設置與目標資訊保密部分對應的識別字，儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；移動終端獲取並向伺服器發送本身的所在地資訊和待識別的識別字；伺服器判斷所述所在地資訊與所述第一位址資訊是否一致，如果一致，則將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。應用本申請，只有當移動終端的所在地資訊與第一位址資訊相同，即送貨人員到達第一位址資訊對應的位址範圍內時，才可以通過識別字獲取對應的保密部分，即得到完整的目標資訊，無論賣家還是商品運輸過程中涉及的其他人員均無法獲取到完整的目標資訊；因此，本申請可以實現對目標資訊的保密，應用於網路購物中，可以達到保護買家隱私的目的。

【圖式簡單說明】

[0044] 為了更清楚地說明本申請實施例或現有技術中的技術方案，下面將對實施例或現有技術描述中所需要使用的附圖作簡單地介紹，顯而易見地，對於本領域普通技術人員而言，在不付出創造性勞動性的前提下，還可以根據這些附圖獲得其他的附圖。

[0045] 圖 1 為本申請實施例提供的一種資訊保密方

法的流程圖；

[0046] 圖 2 為本申請實施例提供的另一種資訊保密方法的流程圖；

[0047] 圖 3 為本申請實施例提供的又一種資訊保密方法的流程圖；

[0048] 圖 4 為本申請實施例提供的又一種資訊保密方法的流程圖；

[0049] 圖 5 為本申請實施例提供的資訊保密系統的結構示意圖；

[0050] 圖 6 為本申請實施例提供的一種伺服器的結構方塊圖；

[0051] 圖 7 為本申請實施例提供的另一種伺服器的結構方塊圖；

[0052] 圖 8 為本申請實施例提供的一種移動終端的結構方塊圖；

[0053] 圖 9 為本申請實施例提供的又一種伺服器的結構方塊圖；

[0054] 圖 10 為本申請實施例提供的另一種移動終端的結構方塊圖。

【實施方式】

[0055] 本申請實施例提供一種資訊保密方法及相關裝置，以解決網路購物過程中買家個人資訊易被洩露的問題。

[0056] 為了使本技術領域的人員更好地理解本申請中的技術方案，下面將結合本申請實施例中的附圖，對本申請實施例中的技術方案進行清楚、完整地描述，顯然，所描述的實施例僅僅是本申請一部分實施例，而不是全部的實施例。基於本申請中的實施例，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，都應當屬於本申請保護的範圍。

[0057] 圖 1 為本申請實施例提供的一種資訊保密方法的流程圖。參照圖 1，該資訊保密方法包括以下步驟：

[0058] S11、伺服器設置與目標資訊保密部分對應的識別字。

[0059] S12、伺服器儲存所述目標資訊保密部分、目標資訊公開部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊。

[0060] 本申請實施例中，伺服器將目標資訊分為兩部分，即公開部分和保密部分，並為每條需要保密的目標資訊保密部分設置一個對應的識別字，然後，一方面儲存目標資訊公開部分、目標資訊保密部分和識別字，另一方面輸出（即公開）所述目標資訊公開部分和所述識別字。

[0061] 上述目標資訊至少包括有效位址資訊，可以將該有效位址資訊分為不需要保密的第一位址資訊和需要保密的第二位址資訊兩部分，即：將第一位址資訊作為目標資訊公開部分，第二位址資訊作為目標資訊保密部分。

[0062] 對於網路購物這一應用場景，訂單建立完成後，伺服器先將買家提供的目標資訊進行上述處理，賣家將接收到的伺服器輸出的目標資訊公開部分和對應的識別字填寫或列印於商品的快遞詳情單上，由物流公司運送該商品。本申請實施例中，賣家只接收到目標資訊公開部分和對應的識別字，並不知道對應的目標資訊保密部分，實現了買家的目標資訊對於賣家的保密。

[0063] 上述有效位址資訊可以為買家的收貨位址；為了不影響物流公司正常送貨，可以將每筆訂單的收貨位址中單位較小的第二位址資訊作為目標資訊保密部分，剩餘的第一位址資訊作為目標資訊公開部分。例如，對於收貨位址“xx 省 xx 市 xx 區 xx 路 xx 號 xx 樓 xx 單元 xx 室”，伺服器可以將單位較小的“xx 單元 xx 室”作為目標資訊保密部分，為其設置識別字 Z，並將目標資訊公開部分“xx 省 xx 市 xx 區 xx 路 xx 號 xx 樓”、目標資訊保密部分“xx 單元 xx 室”和識別字 Z 對應儲存，同時輸出該目標資訊公開部分“xx 省 xx 市 xx 區 xx 路 xx 號 xx 樓”和對應的識別字 Z。需要說明的是，本段所述的目標資訊劃分方式僅僅為本申請的一個具體實施方式，本申請並不局限於上述方式；例如，對於收貨位址“xx 省 xx 市 xx 區 xx 路 xx 號 xx 樓 xx 單元 xx 室”，也可以將“xx 路 xx 號 xx 樓 xx 單元 xx 室” 劃分為目標資訊保密部分，“xx 省 xx 市 xx 區”劃分為目標資訊公開部分。

[0064] 可選的，伺服器中目標資訊及對應的識別字

的儲存形式如下表 1 所示。

[0065]

表 1：目標資訊及識別字

目標資訊公開部分 （包括第一位址資訊）	目標資訊保密部分 （包括第二位址資訊）	識別字
河北省 xx 市 xx 區 xx 路 xx 號 xx 樓	1 單元 202 室	Z1
廣東省 xx 市 xx 區 xx 路 xx 號 xx 樓	1 單元 202 室	Z2
北京市朝陽區安定路安華發展大廈	202 室	Z3
北京市朝陽區安定路安華發展大廈	420 室	Z4
…	…	…
北京市東城區 xx 路 xx 大廈	xx 室	Z7，Z8
…	…	…

[0066] 由表 1 可知，每個識別字都可以唯一確定一個目標資訊。如表 1 中識別字 Z1 和 Z2 對應的目標資訊，雖然其保密部分相同，但由於其公開部分不同，二者一定不是同一目標資訊，故識別字也不同；同理，對於表 1 中識別字 Z3 和 Z4 對應的目標資訊，雖然其公開部分相同，但由於其保密部分不同，二者必然不是同一目標資訊，故對應的識別字也不相同。

[0067] 實際應用中，還可能存在公開部分和保密部分均相同的兩條目標資訊（例如同一買家的兩筆不同的訂單），在本申請一個可行的實施例中，可以為這兩條目標資訊設置同一識別字。但為提高保密性，本申請的一個較佳實施例中，為這兩條目標資訊設置不同的識別字；相應的，可以分別儲存上述兩條目標資訊和對應的識別字，也可以將其合併儲存，如表 1 中目標資訊“北京市東城區

xx 路 xx 大廈 xx 室”存在 Z7 和 Z8 兩個識別字。

[0068] 在本申請的其他可行實施例中，除收貨位址外，目標資訊還可以包括，買家姓名、電話號碼等資訊；為保護買家隱私，上述買家姓名、電話號碼等資訊可以與第一位址資訊共同作為目標資訊保密部分。

[0069] S13、移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器。

[0070] 物流公司的送貨人員在送貨時，可以利用移動終端向伺服器上傳當前的所在地資訊及快遞詳情單上的識別字（即上述待識別的識別字）。其中，可以在上述移動終端中設置 GPS 定位元件，以供移動終端獲取本身的所在地資訊。

[0071] S14、伺服器判斷所述所在地資訊與所述第一位址資訊是否一致。

[0072] S15、如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0073] 伺服器接收到移動終端發送的所在地資訊和待識別的識別字後，在本身的儲存單元中查找該待識別的識別字對應的目標資訊公開部分，即上述第一位址資訊，並將上述所在地資訊與該第一位址資訊進行對比。

[0074] 如果上述所在地資訊與該第一位址資訊相同，說明商品已處於第一位址資訊對應的位址範圍內，同

時說明移動終端的持有者是物流公司的送貨人員，而非位於其他地區的其他人員；此時，伺服器將待識別的識別字對應的目標資訊保密部分（包括上述第二位址資訊）回饋至移動終端，使得送貨人員獲得完整的目標資訊（包括第一位址資訊和第二位址資訊組合而成的有效位址資訊），從而成功將商品送至買家手中。

[0075] 如果上述所在地資訊與該第一位址資訊不相同，伺服器不回饋上述目標資訊保密部分，或者回饋相應的提示資訊，如“位址錯誤”等。

[0076] 由以上技術方案可知本申請實施例提供的資訊保密方法，通過伺服器設置與目標資訊保密部分對應的識別字，儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；移動終端獲取並向伺服器發送本身的所在地資訊和待識別的識別字；伺服器判斷所述所在地資訊與所述第一位址資訊是否一致，如果一致，則將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。應用本申請實施例，只有當移動終端的所在地資訊與第一位址資訊相同，即送貨人員到達第一位址資訊對應的位址範圍內時，才可以通過識別字獲取對應的保密部分，即得到完整的目標資訊，無論賣家還是商品運輸過程中涉及的其他人員均無法獲取到完整的目標資訊；因此，本申請實施例可以實現對目標資訊的保密，應用於網路購物中，可以達到保護買家隱私的

目的。

[0077] 另外，應用本申請實施例，即使出現目標資訊洩露情況，也可以從送貨人員開始追溯責任，充分保障買家的利益。

[0078] 本申請實施例中，除了通過表 1 將目標資訊公開部分和目標資訊保密部分（以及識別字）儲存於伺服器的同一儲存單元中，還可以將目標資訊公開部分和目標資訊保密部分儲存於不同的儲存單元中，屬於同一目標資訊的公開部分和保密部分通過唯一的編號實現關聯。同一目標資訊的不同部分儲存於不同的儲存單元中，使得當伺服器任一儲存單元中的資訊被竊取後，洩露的僅僅是目標資訊的一部分，而不是完整的目標資訊，因此可以進一步提高目標資訊的保密性。

[0079] 上述實施例中，用於關聯目標資訊公開部分和目標資訊保密部分的編號可以採用交易訂單流水號。下表 2 和表 3 示出了本實施例中目標資訊在伺服器中的儲存形式；其中表 2 用於儲存目標資訊公開部分，表 3 用於儲存目標資訊保密部分，表 2 和表 3 儲存於伺服器不同的儲存單元中。

[0080]

表 2：目標資訊公開部分

編號	目標資訊公開部分
2688000111	河北省 xx 市 xx 區 xx 路 xx 號 xx 樓
2688000112	廣東省 xx 市 xx 區 xx 路 xx 號 xx 樓
2688000113	北京市朝陽區安定路安華發展大廈
2688000114	北京市朝陽區安定路安華發展大廈
…	…
2688000117	北京市東城區 xx 路 xx 大廈
…	…

[0081]

表 3：目標資訊保密部分及對應的識別字

編號	目標資訊保密部分	識別字
2688000111	1 單元 202 室	Z1
2688000112	1 單元 202 室	Z2
2688000113	202 室	Z3
2688000114	420 室	Z4
…	…	…
2688000117	xx 室	Z7，Z8
…	…	…

[0082] 如表 2 和表 3 所示，相同的編號對應的目標資訊公開部分和目標資訊保密部分構成一個有效的目標資訊。如編號“2688000111”對應的“河北省 xx 市 xx 區 xx 路 xx 號 xx 樓”和“1 單元 202 室”組合為目標資訊“河北省 xx 市 xx 區 xx 路 xx 號 xx 樓 1 單元 202 室”。

[0083] 根據表 2 和表 3，伺服器接收到移動終端的所在地資訊和待識別的識別字後，獲取對應的第一位址資訊的方法如下：首先在表 3 中查找該待識別的識別字對應的編號，然後在表 2 中查找該編號對應的目標資訊公開部

分，查找到的目標資訊公開部分即為該待識別的識別字對應的第一位址資訊。

[0084] 在本申請一個可行的實施例中，伺服器設置與目標資訊保密部分對應的識別字，可以為：伺服器根據預設加密規則對所述目標資訊保密部分進行加密處理，得到所述識別字。實際應用中，不同類型的識別字可以採用不同的預設加密規則，例如：根據二維碼編碼規則生成與目標資訊保密部分對應的二維碼、根據條碼編碼規則生成與目標資訊保密部分對應的條碼。

[0085] 本申請實施例中，識別字的具體類型多種多樣，可以採用以下一種或多種：二維碼、條碼、射頻識別（Radio Frequency Identification，RFID）碼、字串等。

[0086] 若採用二維碼或條碼作為識別字，賣家可以直接將該二維碼或條碼列印於商品的快遞詳情單上；相應的，上述移動終端可以為專業掃碼設備，也可以為具有相應掃碼功能的其他電子設備，例如可以利用智慧手機掃描二維碼。

[0087] 若採用射頻識別碼作為識別字，則賣家可以將儲存有該射頻識別碼的 RFID 晶片（又稱電子標籤）粘貼於商品的快遞詳情單上，相應的，上述移動終端可以為 RFID 閱讀器，也可以為具有射頻識別功能的其他電子設備，其通過天線與 RFID 晶片進行無線通訊，以讀取 RFID 晶片中儲存的射頻識別碼。

[0088] 若採用字串作為識別字，賣家可以直接將字

串填寫或列印於商品的快遞詳情單上，相應的，可以透過移動終端上的實體鍵盤或虛擬鍵盤輸入上述字串。上述字串可以為數位串、漢字串、字母串、特殊符號串，或者包含數位、漢字、字母和特殊符號中的至少兩種的組合字串。

[0089] 圖 2 為本申請實施例提供的另一種資訊保密方法的流程圖。參照圖 2，該資訊保密方法包括以下步驟：

[0090] S21、伺服器設置與目標資訊保密部分對應的識別字。

[0091] S22、伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊。

[0092] S23、移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器。

[0093] S24、伺服器判斷所述所在地資訊與所述第一位址資訊是否一致。

[0094] S25、如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0095] 上述步驟 S21 至 S25 分別與前文實施例所述的步驟 S11 至 S15 對應，此處不再贅述。

[0096] S26、伺服器刪除本身儲存的與所述待識別的識別字對應的目標資訊保密部分。

[0097] 仍以表 1 為例，如果步驟 S25 中伺服器將識別字 Z4 對應的目標資訊保密部分“420 室”發送至移動終端，則在 S26 中，伺服器刪除該目標資訊保密部分“420 室”。

[0098] 進一步的，伺服器還可以同時刪除本身儲存的與所述待識別的識別字相關的所有資訊，例如，在刪除目標資訊保密部分“420 室”的同時，還可以刪除對應的目標資訊公開部分“北京市朝陽區安定路安華發展大廈”，以及識別字“Z4”，即刪除序號 4 的整行資訊。

[0099] 本申請實施例中，在將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器刪除本身的儲存單元中與上述待識別的識別字對應的目標資訊保密部分，使得移動終端不能再次透過該識別字獲取對應的目標資訊保密部分，進一步提高了目標資訊的保密性。

[0100] 在本申請另一個可行的實施例中，在伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器還可以將本身儲存的與所述待識別的識別字相同的識別字為無效識別字，如下表 4 所示，同樣使得移動終端不能再次通過該識別字獲取對應的目標資訊保密部分，進一步提高了目標資訊的保密性。

[0101]

表 4：目標資訊保密部分及對應的識別字

編號	目標資訊保密部分	識別字	狀態
2688000111	1 單元 202 室	Z1	無效
2688000112	1 單元 202 室	Z2	有效
…	…	…	…

[0102] 圖 3 為本申請實施例提供的又一種資訊保密方法的流程圖，應用於伺服器。參見圖 3，該資訊保密方法包括：

[0103] S31、伺服器設置與目標資訊保密部分對應的識別字。

[0104] S32、伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊。

[0105] S33、伺服器接收移動終端發送的所在地資訊和待識別的識別字。

[0106] S34、伺服器判斷所述所在地資訊與所述第一位址資訊是否一致。

[0107] S35、如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0108] 由以上技術方案可知，本申請實施例提供的資訊保密方法，通過伺服器設置與目標資訊保密部分對應的識別字，儲存所述目標資訊公開部分、目標資訊保密部

分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；移動終端獲取並向伺服器發送本身的所在地資訊和待識別的識別字；伺服器判斷所述所在地資訊與所述第一位址資訊是否一致，如果一致，則將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。應用本申請實施例，只有當接收到的移動終端的所在地資訊與第一位址資訊相同時，才可以將對應的目標資訊保密部分回饋至移動終端，使得移動終端得到完整的目標資訊，無論賣家還是商品運輸過程中涉及的其他人員均無法獲取到完整的目標資訊；因此，本申請實施例可以實現對目標資訊的保密，應用於網路購物中，可以達到保護買家隱私的目的。

[0109] 在本申請的另一可行實施例中，伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，還可以執行如下步驟：

[0110] 伺服器刪除本身儲存的與所述待識別的識別字對應的目標資訊保密部分，或者，將本身儲存的與所述待識別的識別字相同的識別字為無效識別字。

[0111] 透過執行上述步驟，實現了識別字單次有效，使得移動終端不能再次透過該識別字獲取對應的目標資訊保密部分，進一步提高了目標資訊的保密性。

[0112] 可選的，圖 3 所述實施例中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0113] 可選的，圖 3 所述實施例中，所述目標資訊

保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0114] 可選的，圖 3 所述實施例中，所述伺服器設置與目標資訊保密部分對應的識別字，包括：伺服器根據預設加密規則對所述目標資訊保密部分進行加密處理，得到所述識別字。

[0115] 圖 4 為本申請實施例提供的又一種資訊保密方法的流程圖，應用於移動終端。參見圖 4，該資訊保密方法包括：

[0116] S41、移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器。

[0117] S42、移動終端接收伺服器發送的目標資訊保密部分。

[0118] 本申請實施例中，伺服器按照以下方式向移動終端回饋資訊：判斷移動終端發送的所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果上述所在地資訊與所述第一位址資訊一致，則將待識別的識別字對應的目標資訊保密部分發送至移動終端。相反的，如果上述所在地資訊與所述第一位址資訊不一致，則伺服器不向移動終端發送對應的目標資訊保密部分，或者向移動終端發送“位址錯誤”等提示資訊。

[0119] 由以上技術方案可知，當且僅當移動終端隨送貨人員進入第一位址資訊對應的位址範圍內時，才可以

從伺服器中獲取到完整的目標資訊，而無論賣家還是商品運輸過程中涉及的其他人員均無法獲取到完整的目標資訊；因此，本申請實施例可以實現對目標資訊的保密，應用於網路購物中，可以達到保護買家隱私的目的。

[0120] 可選的，圖 4 所述實施例中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0121] 可選的，圖 4 所述實施例中，所述目標資訊保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0122] 圖 5 為本申請實施例提供的資訊保密系統的方塊圖，該資訊保密系統包括伺服器 500 和移動終端 600。

[0123] 圖 6 為本申請實施例提供的一種伺服器 500 的結構方塊圖。參見圖 5，該伺服器 500 包括：設置單元 501、儲存單元 502、輸出單元 503、接收單元 504、判斷單元 505 和發送單元 506。

[0124] 其中，該設置單元 501 被配置為：設置與目標資訊保密部分對應的識別字。

[0125] 該儲存單元 502 被配置為：儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字。所述目標資訊公開部分至少包括第一位址資訊。

[0126] 該輸出單元 503 被配置為：輸出所述目標資訊公開部分和所述識別字。

[0127] 該接收單元 504 被配置為：接收移動終端發

送的所在地資訊和待識別的識別字。

[0128] 該判斷單元 505 被配置為：判斷所述所在地資訊與所述第一位址資訊是否一致。

[0129] 該發送單元 506 被配置為：在所述所在地資訊與所述第一位址資訊一致時，將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0130] 如圖 7 所示，在本申請的另一可行的實施例中，伺服器 500 還可以包括：更新單元 507。該更新單元 507 被配置為：在將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，刪除所述儲存單元中與所述待識別的識別字對應的目標資訊保密部分。

[0131] 圖 8 為本申請實施例提供的一種移動終端 600 的結構方塊圖。參見圖 8，該移動終端 600 包括：獲取單元 601、發送單元 602 和接收單元 603。

[0132] 該獲取單元 601 被配置為：獲取移動終端的所在地資訊和待識別的識別字；

[0133] 該發送單元 602 被配置為：將所述所在地資訊和待識別的識別字發送至伺服器；

[0134] 該接收單元 603 被配置為：接收伺服器按照以下方式回饋的資訊：伺服器判斷所述所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0135] 關於上述實施例中的裝置，其中各個單元執

行操作的具體方式已經在有關該方法的實施例中進行了詳細描述，此處將不做詳細闡述說明。

[0136] 圖 9 為本申請實施例提供的又一種伺服器 500 的結構方塊圖；參照圖 9，伺服器 500 包括處理元件 510，其進一步包括一個或多個處理器，以及由記憶體 520 所代表的記憶體資源，用於儲存可由處理元件 510 的執行的指令，例如應用程式。記憶體 520 中儲存的應用程式可以包括一個或一個以上的每一個對應於一組指令的模組。此外，處理元件 510 被配置為執行指令，以執行上述資訊保密方法。

[0137] 伺服器 500 還可以包括電源元件 550、網路介面 540 和輸入輸出介面 530。其中，電源元件 550 被配置為執行伺服器 500 的電源管理；網路介面 540 可以為有線網路介面或無線網路介面 540，被配置為將伺服器 500 連接到網路。伺服器 500 可以操作基於儲存在記憶體 520 的作業系統，例如 Windows ServerTM、Mac OS XTM、UnixTM、LinuxTM、FreeBSDTM 或類似。

[0138] 本申請實施例還提供了一種包括指令的非臨時性電腦可讀儲存介質，例如伺服器 500 中的記憶體 520，上述指令可由伺服器 500 的處理器執行以完成上述方法。例如，所述非臨時性電腦可讀儲存介質可以是 ROM、隨機存取記憶體（RAM）、CD-ROM、磁帶、軟碟和光資料存放裝置等。

[0139] 當所述非臨時性電腦可讀儲存介質中的指令

由伺服器 500 的處理器執行時，使得該伺服器 500 能夠執行一種輸入方法，所述方法包括：

[0140] 伺服器設置與目標資訊保密部分對應的識別字；伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；伺服器接收移動終端發送的所在地資訊和待識別的識別字；伺服器判斷所述所在地資訊與所述第一位址資訊是否一致；如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0141] 在本申請一個可行的實施例中，所述方法還包括：在將所述待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器刪除本身儲存的與所述待識別的識別字對應的目標資訊保密部分。

[0142] 在本申請另一個可行的實施例中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0143] 在本申請又一個可行的實施例中，所述目標資訊保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0144] 在本申請又一個可行的實施例中，所述伺服器設置與目標資訊保密部分對應的識別字，包括：伺服器

根據預設加密規則對所述目標資訊保密部分進行加密處理，得到所述識別字。

[0145] 圖 10 為本申請實施例提供的一種移動終端 600 的結構方塊圖；該移動終端 600 可以是手機、平板設備、電腦等。

[0146] 參見圖 10，本申請實施例提供的移動終端 600 可以包括以下一個或多個元件：處理元件 610、記憶體 620、通信元件 630、電源元件 640、感測器元件 650、輸入/輸出（I/O）介面 660、多媒體元件 670 和音訊元件 680。

[0147] 其中，處理元件 610 通常控制移動終端的整體操作，諸如與顯示、電話呼叫、資料通信、相機操作和記錄操作相關聯的操作。處理元件 610 可以包括一個或多個處理器 611 來執行本地或者遠端指令，以完成上述實施例所述方法的全部或部分步驟。此外，處理元件 610 可以包括一個或多個模組，便於處理元件 610 和其他元件之間的交互。例如，處理元件 610 可以包括多媒體模組，以方便多媒體元件 670 和處理元件 610 之間的交互。

[0148] 記憶體 620 被配置為儲存各種類型的資料以支援在移動終端上的操作。這些資料的示例包括用於在移動終端上操作的任何應用程式或方法的指令、連絡人資料、電話簿資料、消息、圖片、視頻等。記憶體 620 可以由任何類型的揮發性或非揮發性存放裝置或者它們的組合實現，如靜態隨機存取記憶體（SRAM），電可抹除可程

式設計唯讀記憶體（EEPROM），可抹除可程式設計唯讀記憶體（EPROM），可程式設計唯讀記憶體（PROM），唯讀記憶體（ROM），磁記憶體，快閃記憶體，磁片或光碟。

[0149] 通信元件 630 被配置為便於所述移動終端和其他設備之間有線或無線方式的通信。所述移動終端可以接入基於通信標準的無線網路，如 Wi-Fi，2G 或 3G，或它們的組合。在一個示例性實施例中，通信元件 630 經由廣播通道接收來自外部廣播管理系統的廣播信號或廣播相關資訊。在一個示例性實施例中，所述通信元件 630 還包括近場通信（NFC）模組，以促進短程通信。例如，在 NFC 模組可基於射頻識別（RFID）技術，紅外數據協會（IrDA）技術，超寬頻（UWB）技術，藍牙（bluetooth）技術和其他技術來實現。

[0150] 電源元件 640 為所述移動終端的各種元件提供電力。電源元件 640 可以包括電源管理系統，一個或多個電源，及其他與為所述移動終端生成、管理和分配電力相關聯的組件。

[0151] 感測器元件 650 包括一個或多個感測器，用於為所述移動終端提供各個方面的狀態評估。例如，感測器元件 650 可以檢測到所述移動終端的打開/關閉狀態、元件（所述移動終端的顯示器和小鍵盤等）的相對定位，感測器元件 650 還可以檢測所述移動終端或所述移動終端一個元件的位置改變、使用者與所述移動終端接觸的存在

或不存在、所述移動終端方位或加速/減速和所述移動終端的溫度變化。感測器元件 650 可以包括接近感測器，被配置用來在沒有任何的物理接觸時檢測附近物體的存在。感測器元件 650 還可以包括光感測器，如 CMOS 或 CCD 影像感測器，用於在成像應用中使用。在一些實施例中，該感測器元件 650 還可以包括加速度感測器，陀螺儀感測器，磁感測器，壓力感測器或溫度感測器。在一些實施例中，感測器元件 650 還可以包括前置鏡頭和/或後置鏡頭。當所述移動終端處於操作模式，如拍攝模式或視訊模式時，前置鏡頭和/或後置鏡頭可以接收外部的資料。每個前置鏡頭和後置鏡頭可以是一個固定的光學透鏡系統或具有焦距和光學變焦能力。

[0152] 輸入/輸出元件 660 為處理元件 610 和週邊介面模組之間提供介面，上述週邊介面模組可以是鍵盤，點擊輪，按鈕等。這些按鈕可包括但不限於：主頁按鈕、音量按鈕、啟動按鈕和鎖定按鈕。

[0153] 多媒體元件 670 包括在所述移動終端和使用者之間提供的一個輸出介面的螢幕。在一些實施例中，螢幕可以包括液晶顯示器（LCD）和觸控面板（TP）。如果螢幕包括觸控面板，螢幕可以被實現為觸控式螢幕，以接收來自使用者的輸入信號。觸控面板包括一個或多個觸控感測器以感測觸控、滑動和觸控面板上的手勢。所述觸控感測器可以不僅感測觸控或滑動動作的邊界，而且還檢測與所述觸控或滑動操作相關的持續時間和壓力。

[0154] 音訊元件 680 被配置為輸出和/或輸入音訊信號。例如，音訊元件 680 包括一個麥克風（MIC），當所述移動終端處於操作模式，如呼叫模式、記錄模式和語音辨識模式時，麥克風被配置為接收外部音訊信號。所接收的音訊信號可以被進一步儲存在記憶體 620 或經由通信元件 630 發送。在一些實施例中，音訊元件 680 還包括一個揚聲器，用於輸出音訊信號。

[0155] 本申請實施例中，所述移動終端可以被一個或多個特殊用途積體電路（ASIC）、數位訊號處理器（DSP）、數位信號處理設備（DSPD）、可程式設計邏輯器件（PLD）、現場可程式設計閘陣列（FPGA）、控制器、微控制器、微處理器或其他電子元件實現，用於執行上述方法。

[0156] 本申請實施例還提供了一種包括指令的非臨時性電腦可讀儲存介質，例如包括指令的記憶體 620，上述指令可由移動終端的處理器 611 執行以完成上述方法。例如，所述非暫態電腦可讀儲存介質可以是 ROM、隨機存取記憶體（RAM）、CD-ROM、磁帶、軟碟和光資料存放裝置等。

[0157] 當所述非暫態電腦可讀儲存介質中的指令由移動終端的處理器執行時，使得該移動終端能夠執行一種輸入方法，所述方法包括：

[0158] 移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺

服器；移動終端接收伺服器按照以下方式回饋的目標資訊保密部分：伺服器判斷所述所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果所述所在地資訊與所述第一位址資訊一致，則伺服器將待識別的識別字對應的目標資訊保密部分發送至移動終端。

[0159] 在本申請一個可行的實施例中，所述識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

[0160] 在本申請又一個可行的實施例中，所述目標資訊保密部分包括第二位址資訊；其中，所述第一位址資訊和第二位址資訊的組合為所述目標資訊中的有效位址資訊。

[0161] 需要說明的是，在本文中，諸如“第一”和“第二”等之類的關係術語僅僅用來將一個實體或者操作與另一個實體或操作區分開來，而不一定要求或者暗示這些實體或操作之間存在任何這種實際的關係或者順序。而且，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、物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、物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、物品或者設備中還存在另外的相同要素。

[0162] 以上所述僅是本申請的具體實施方式，使本領域技術人員能夠理解或實現本申請。對這些實施例的多

種修改對本領域的技術人員來說將是顯而易見的，本文中所定義的一般原理可以在不脫離本申請的精神或範圍的情況下，在其它實施例中實現。因此，本申請將不會被限制於本文所示的這些實施例，而是要符合與本文所公開的原理和新穎特點相一致的最寬的範圍。

【符號說明】

[0163]

500：伺服器

501：設置單元

502：儲存單元

503：輸出單元

504：接收單元

505：判斷單元

506：發送單元

507：更新單元

510：處理元件

520：記憶體

530：輸入輸出介面

540：網路介面

550：電源元件

600：移動終端

601：獲取單元

602：發送單元

603：接收單元

610：處理元件

620：記憶體

630：通信元件

640：電源元件

650：感測器元件

660：輸入/輸出介面

670：多媒體元件

680：音訊元件

611：處理器

公告本

I632484

發明摘要

※申請案號：103134017

※申請日：103 年 09 月 30 日　　※IPC 分類：

【發明名稱】(中文/英文)

資訊保密方法及相關裝置

【中文】

本申請實施例公開了一種資訊保密方法及相關裝置，通過伺服器設置與目標資訊保密部分對應的識別字，儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊；移動終端獲取並向伺服器發送本身的所在地資訊和待識別的識別字；伺服器判斷所述所在地資訊與所述第一位址資訊是否一致，如果一致，則將所述待識別的識別字對應的目標資訊保密部分發送至移動終端。應用本申請，只有當移動終端的所在地資訊與第一位址資訊相同，即送貨人員到達第一位址資訊對應的位址範圍內時，移動終端才可以得到完整的目標資訊，因此，本申請可以實現對目標資訊的保密。

【英文】

圖式

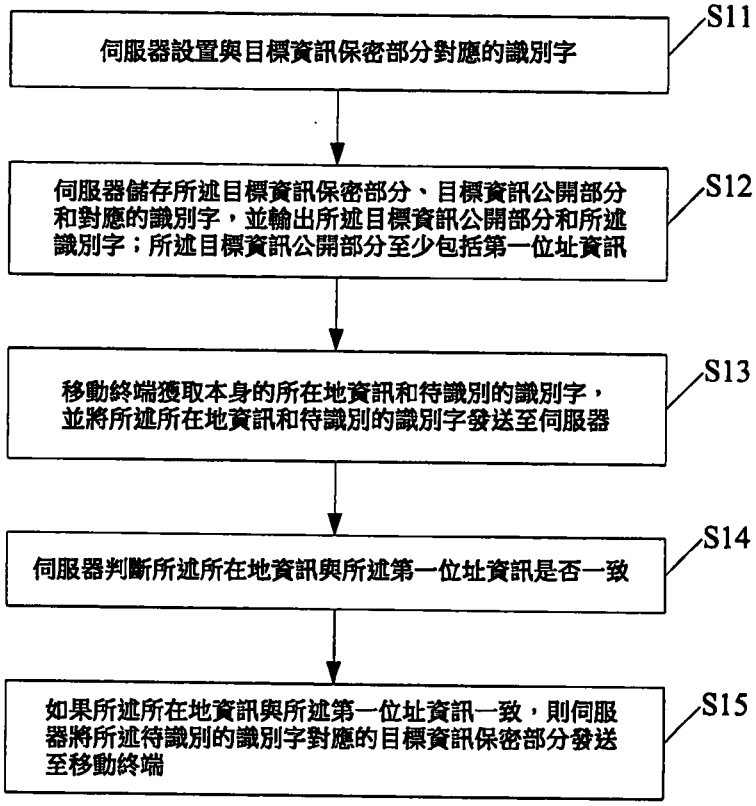
伺服器設置與目標資訊保密部分對應的識別字
S11
伺服器儲存所述目標資訊保密部分、目標資訊公開部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊
S12
移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器
S13
伺服器判斷所述所在地資訊與所述第一位址資訊是否一致
S14
如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端
S15

圖 1

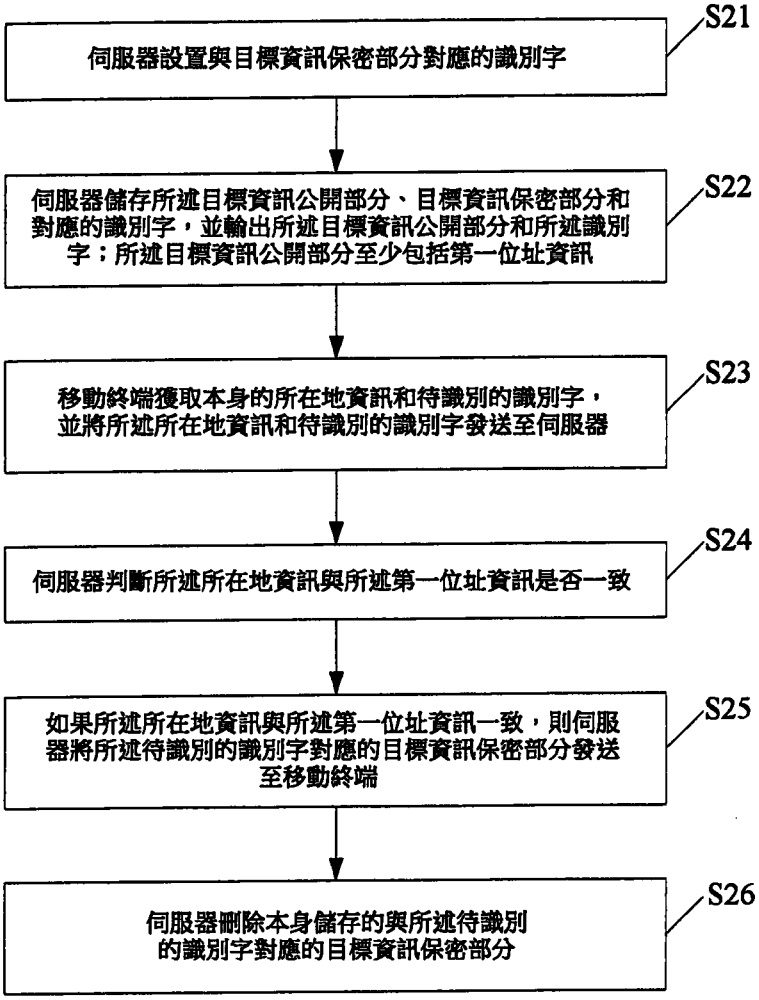
伺服器設置與目標資訊保密部分對應的識別字
S21
伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊
S22
移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器
S23
伺服器判斷所述所在地資訊與所述第一位址資訊是否一致
S24
如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端
S25
伺服器刪除本身儲存的與所述待識別的識別字對應的目標資訊保密部分
S26

圖 2

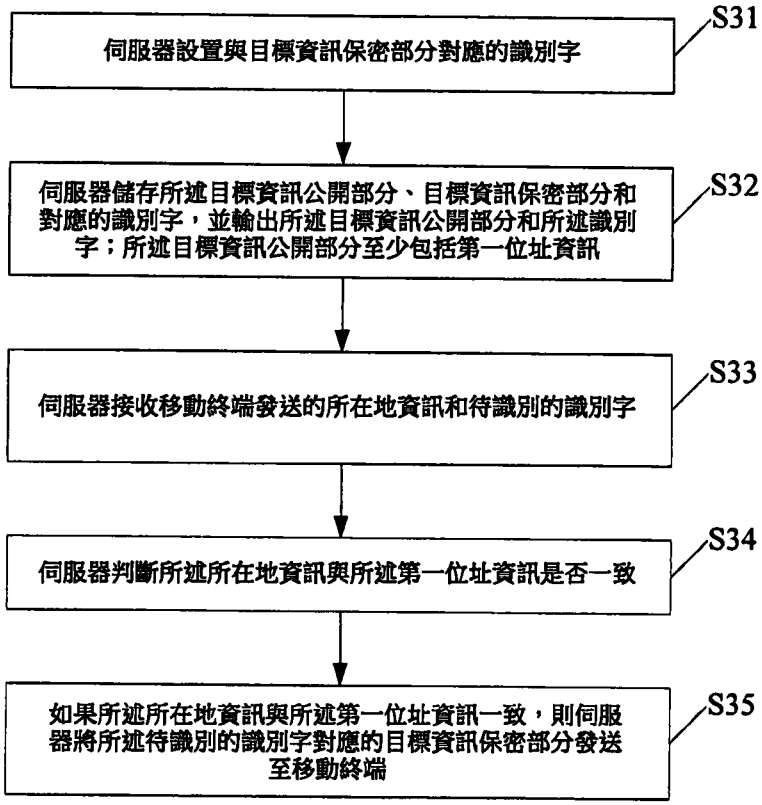
伺服器設置與目標資訊保密部分對應的識別字
S31
伺服器儲存所述目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和所述識別字；所述目標資訊公開部分至少包括第一位址資訊
S32
伺服器接收移動終端發送的所在地資訊和待識別的識別字
S33
伺服器判斷所述所在地資訊與所述第一位址資訊是否一致
S34
如果所述所在地資訊與所述第一位址資訊一致，則伺服器將所述待識別的識別字對應的目標資訊保密部分發送至移動終端
S35

圖 3

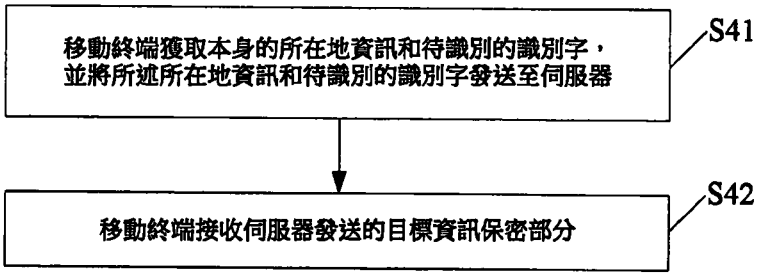
移動終端獲取本身的所在地資訊和待識別的識別字，並將所述所在地資訊和待識別的識別字發送至伺服器
S41
移動終端接收伺服器發送的目標資訊保密部分
S42

圖 4

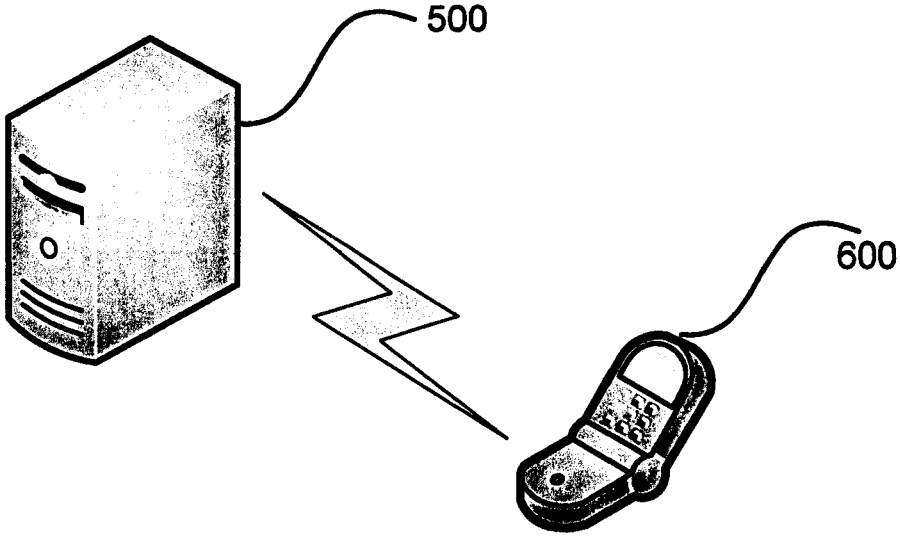
500
600

圖 5

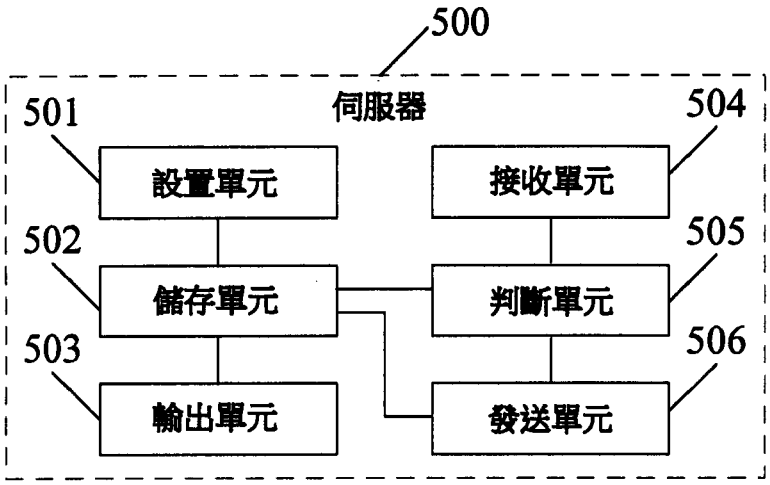
500
伺服器
501
設置單元
502
儲存單元
503
輸出單元
504
接收單元
505
判斷單元
506
發送單元

圖 6

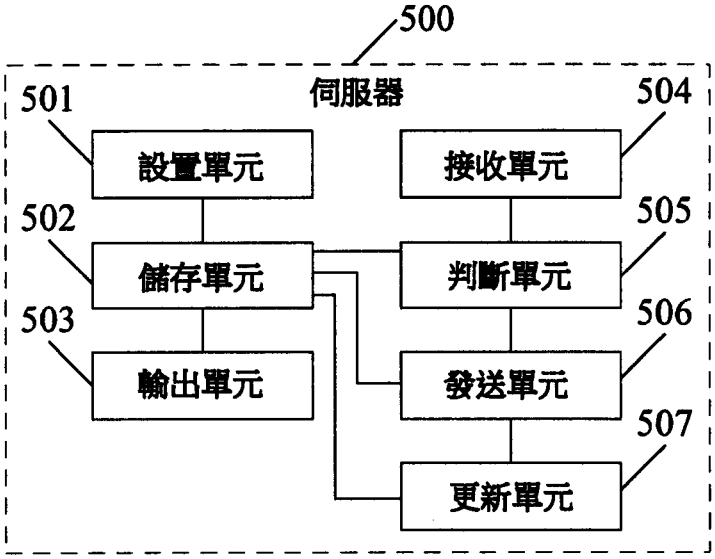
500
伺服器
501
設置單元
502
儲存單元
503
輸出單元
504
接收單元
505
判斷單元
506
發送單元
507
更新單元

圖 7

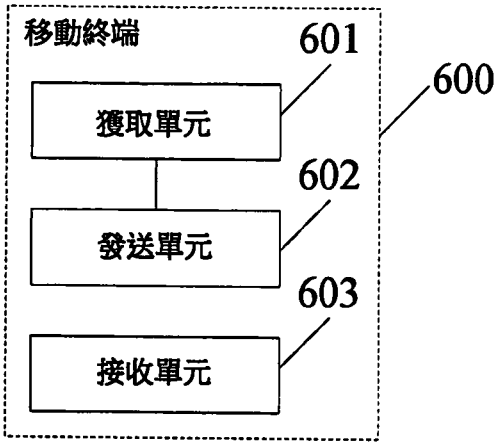
移動終端
601
600
獲取單元
602
發送單元
603
接收單元

圖 8

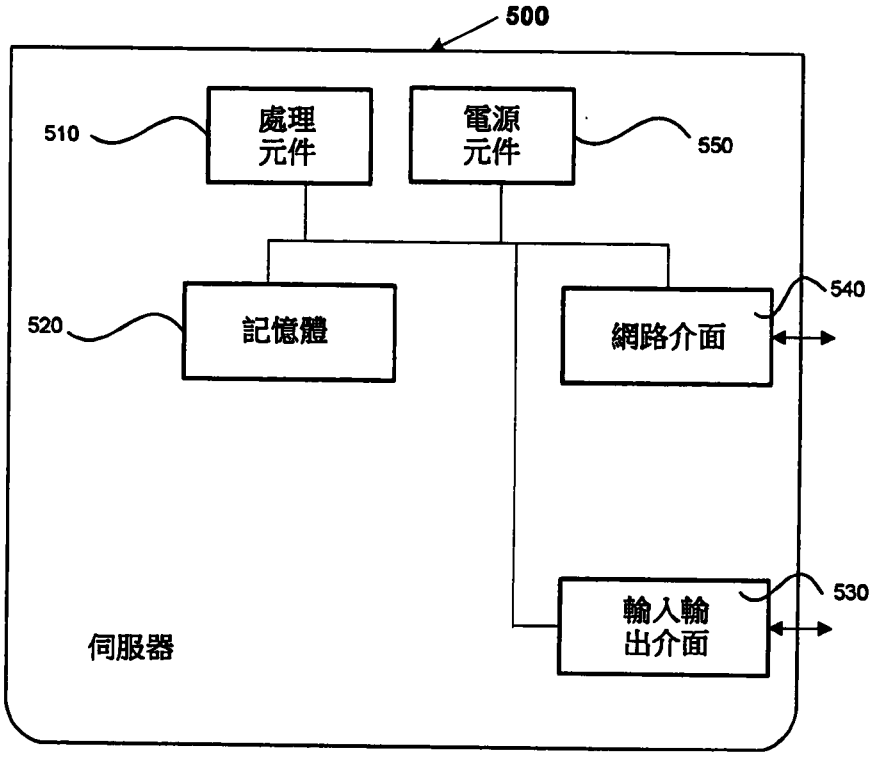
500
510
處理元件
電源元件
550
520
記憶體
網路介面
540
輸入輸出介面
530
伺服器

圖 9

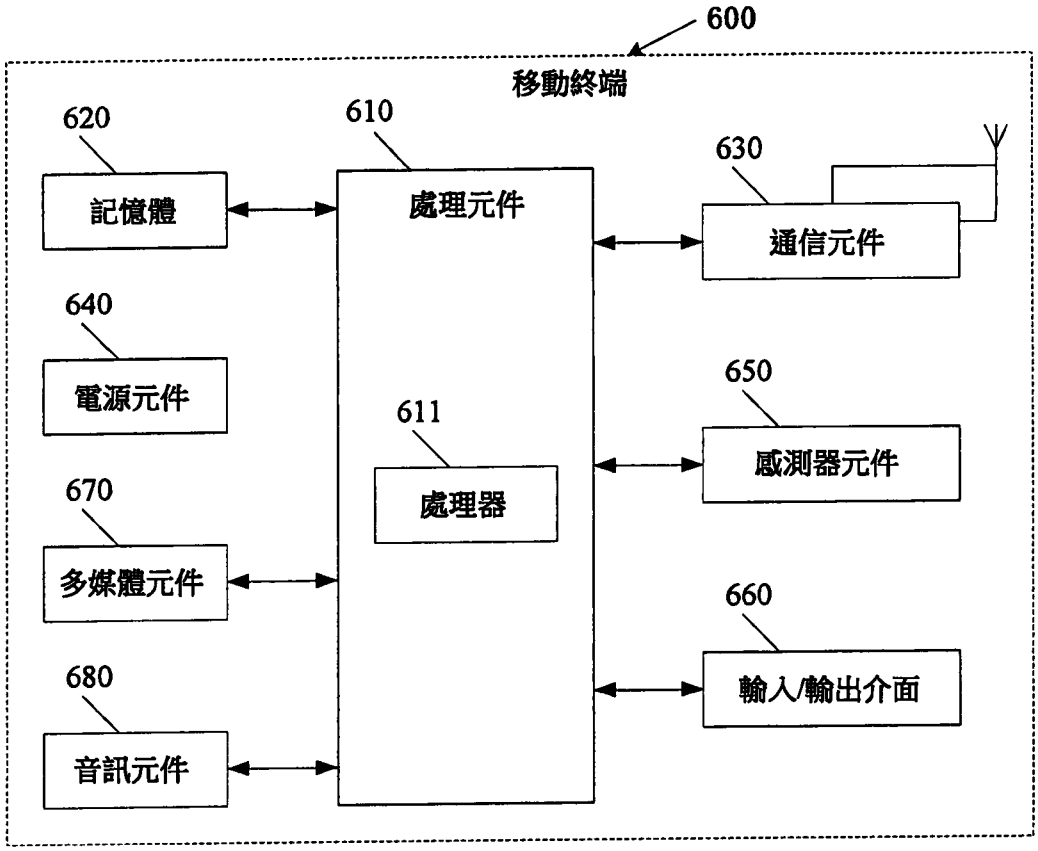
600
移動終端
620
記憶體
610
處理元件
611
處理器
630
通信元件
640
電源元件
650
感測器元件
670
多媒體元件
660
輸入/輸出介面
680
音訊元件

圖 10

【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

申請專利範圍

1.一種資訊保密方法，其特徵在於，包括：

伺服器設置與目標資訊保密部分對應的識別字；

伺服器儲存該目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出所述目標資訊公開部分和該識別字；該目標資訊公開部分至少包括第一位址資訊；

移動終端獲取本身的所在地資訊和待識別的識別字，並將該所在地資訊和待識別的識別字發送至伺服器；

伺服器判斷該所在地資訊與該第一位址資訊是否一致；

如果該所在地資訊與該第一位址資訊一致，則伺服器將該待識別的識別字對應的目標資訊保密部分發送至移動終端，

其中，該識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

2.根據申請專利範圍第 1 項所述的資訊保密方法，其中，還包括：

在將該待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器刪除本身儲存的與該待識別的識別字對應的目標資訊保密部分。

3.根據申請專利範圍第 1 或 2 項所述的資訊保密方法，其中，該目標資訊保密部分包括第二位址資訊；

其中，該第一位址資訊和第二位址資訊的組合為該目標資訊中的有效位址資訊。

4.根據申請專利範圍第 1 或 2 項所述的資訊保密方法，其中，該伺服器設置與目標資訊保密部分對應的識別字，包括：

伺服器根據預設加密規則對該目標資訊保密部分進行加密處理，得到該識別字。

5.一種資訊保密方法，其特徵在於，包括：

伺服器設置與目標資訊保密部分對應的識別字；

伺服器儲存該目標資訊公開部分、目標資訊保密部分和對應的識別字，並輸出該目標資訊公開部分和該識別字；該目標資訊公開部分至少包括第一位址資訊；

伺服器接收移動終端發送的所在地資訊和待識別的識別字；

伺服器判斷該所在地資訊與該第一位址資訊是否一致；

如果該所在地資訊與該第一位址資訊一致，則伺服器將該待識別的識別字對應的保密部分發送至移動終端，

其中，該識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

6.根據申請專利範圍第 5 項所述的資訊保密方法，其中，還包括：

在將該待識別的識別字對應的目標資訊保密部分發送至移動終端後，伺服器刪除本身儲存的與該待識別的識別字對應的目標資訊保密部分。

7.根據申請專利範圍第 5 或 6 項所述的資訊保密方

法，其中，該目標資訊保密部分包括第二位址資訊；

其中，該第一位址資訊和第二位址資訊的組合為該目標資訊中的有效位址資訊。

8.根據申請專利範圍第 5 或 6 項所述的資訊保密方法，其中，該伺服器設置與目標資訊保密部分對應的識別字，包括：

伺服器根據預設加密規則對該目標資訊保密部分進行加密處理，得到該識別字。

9.一種資訊保密方法，其特徵在於，包括：

移動終端獲取本身的所在地資訊和待識別的識別字，並將該所在地資訊和待識別的識別字發送至伺服器；

移動終端接收伺服器按照以下方式回饋的目標資訊保密部分：伺服器判斷該所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果該所在地資訊與該第一位址資訊一致，則伺服器將待識別的識別字對應的目標資訊保密部分發送至移動終端，

其中，該識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

10.根據申請專利範圍第 9 項所述的資訊保密方法，其中，該目標資訊保密部分包括第二位址資訊；

其中，該第一位址資訊和第二位址資訊的組合為該目標資訊中的有效位址資訊。

11.一種伺服器，其特徵在於，包括：

設置單元，用於設置與目標資訊保密部分對應的識別

字；

儲存單元，用於儲存該目標資訊公開部分、目標資訊保密部分和對應的識別字；該目標資訊公開部分至少包括第一位址資訊；

輸出單元，用於輸出該目標資訊公開部分和該識別字；

接收單元，用於接收移動終端發送的所在地資訊和待識別的識別字；

判斷單元，用於判斷該所在地資訊與該第一位址資訊是否一致；

發送單元，用於在該所在地資訊與該第一位址資訊一致時，將該待識別的識別字對應的目標資訊保密部分發送至移動終端，其中，該識別字包括以下至少一種：二維碼、條碼、射頻識別碼和字串。

12.一種移動終端，其特徵在於，包括：

獲取單元，用於獲取移動終端的所在地資訊和待識別的識別字；

發送單元，用於將該所在地資訊和待識別的識別字發送至伺服器；

接收單元，用於接收伺服器按照以下方式回饋的目標資訊保密部分：伺服器判斷該所在地資訊與目標資訊公開部分中的第一位址資訊是否一致，如果該所在地資訊與該第一位址資訊一致，則伺服器將該待識別的識別字對應的目標資訊保密部分發送至移動終端，其中，該識別字包括

以下至少一種：二維碼、條碼、射頻識別碼和字串。