I756266

(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 I756266 B**

(45)公告日： 中華民國 111 (2022) 年 03 月 01 日

(21)申請案號：106132402 (22)申請日： 中華民國 106 (2017) 年 09 月 21 日

(51)Int. Cl.： ***G06F21/31 (2013.01)***

(30)優先權：2016/12/08 中國大陸 201611125263.0

(71)申請人：開曼群島商創新先進技術有限公司 (開曼群島) ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)
開曼群島

(72)發明人：修超 (CN) ；王磊 (CN) ；陳星 (CN) ；李傳智 (CN) ；張永志 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 101895542B CN 106156597A

CN 102075507A

審查人員：馮聖原

申請專利範圍項數：8 項 圖式數：5 共 29 頁

(54)名稱

基於驗證碼的檢查方法及裝置

(57)摘要

本發明實施例揭示了一種基於驗證碼的檢查方法及裝置。該方法包括：接收檢查請求，當接收到所述檢查請求後，獲取預先產生的第一字串；其中，所述第一字串中包含至少一個可變字元，根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串，根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查。利用本發明實施例，可以能夠增加用戶辨識驗證碼的準確性，減少檢查過程的耗時，同時，增加了電腦程式對驗證碼的識別難度，也能夠有效降低電腦程式執行非法操作的可能。

指定代表圖：

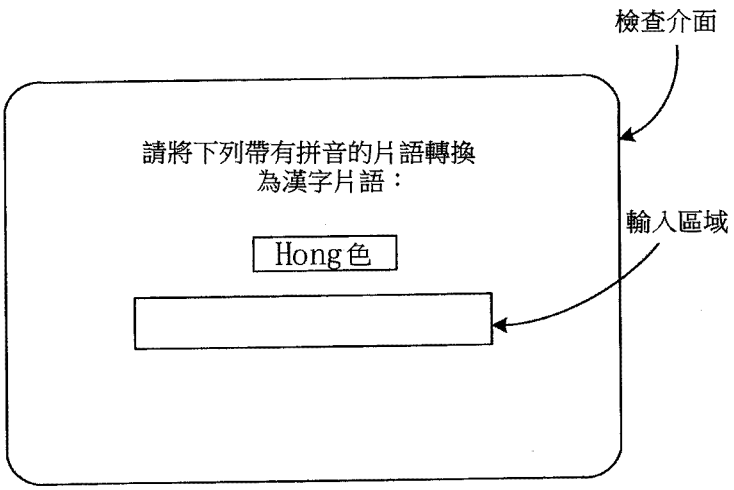

圖 4a

專利案號：106132402

公告本

I756266

【發明摘要】

【中文發明名稱】

基於驗證碼的檢查方法及裝置

【中文】

本發明實施例揭示了一種基於驗證碼的檢查方法及裝置。該方法包括：接收檢查請求，當接收到所述檢查請求後，獲取預先產生的第一字串；其中，所述第一字串中包含至少一個可變字元，根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串，根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查。利用本發明實施例，可以能夠增加用戶辨識驗證碼的準確性，減少檢查過程的耗時，同時，增加了電腦程式對驗證碼的識別難度，也能夠有效降低電腦程式執行非法操作的可能。

【指定代表圖】第(4a)圖。

【代表圖之符號簡單說明】無

【特徵化學式】無

第 106132402 號　　民國 108 年 6 月 28 日修正

【發明說明書】

【中文發明名稱】

基於驗證碼的檢查方法及裝置

【技術領域】

本發明關於電腦技術領域，尤其關於一種基於驗證碼的檢查方法及裝置。

【先前技術】

目前，驗證碼（Completely Automated Public Turing test to tell Computers and Humens Apart, CAPTCHA，也稱為全自動區分電腦和人類的圖靈測試）作為一種安全檢查方式，得到了廣泛應用，其中，驗證碼可以區分操作者是用戶個人還是非法程式，透過驗證碼可防止諸如：惡意嘗試登錄用戶帳戶、枚舉式破解用戶密碼、或者利用腳本控制進行刷單、發言等非法操作。

現有技術中，為了防止非法程式對驗證碼的自動識別，驗證碼所採用的展示方式越來越複雜多變，通常採用如下方式進行展示：方式一，如圖1a所示，驗證碼使用數字或文字表達，並在驗證碼展示區中增加背景，或針對數字或文字進行扭曲，以便增強驗證碼的干擾程度。方式二，如圖1b所示，提供多張圖片以及提示資訊，使得用戶基於提示資訊從多張相似的圖片中識別出相應數量的特定圖片。

然而，在上述的方式中，驗證碼採用較為複雜的展示方式，雖然能夠對非法腳本自動識別起到干擾作用，但同樣也增加了對用戶的干擾，換言之，當上述的驗證碼展示給用戶後，用戶識別錯誤的概率會增加，一旦出錯，用戶需要刷新驗證碼，並繼續對新產生的驗證碼進行識別，直到透過檢查。顯然，現有技術中的上述檢查過程可能需要耗費較長的時間，特別是在識別出錯的情況下，將導致用戶需重複進行檢查。

【發明內容】

本發明實施例提供一種基於驗證碼的檢查方法，用以解決現有技術中用戶對驗證碼識別出錯可能性較大導致檢查過程耗時較長的問題。

本發明實施例提供一種基於驗證碼的檢查裝置，用以解決現有技術中用戶對驗證碼識別出錯可能性較大導致檢查過程耗時較長的的問題。

本發明實施例採用下述技術方案：

本發明實施例提供的一種基於驗證碼的檢查方法，包括：

接收檢查請求；

當接收到所述檢查請求後，獲取預先產生的第一字串；其中，所述第一字串中包含至少一個可變字元；

根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串；

根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查。

本發明實施例提供的一種基於驗證碼的檢查裝置，包括：

接收模組，接收檢查請求；

獲取模組，當接收到所述檢查請求後，獲取預先產生的第一字串；其中，所述第一字串中包含至少一個可變字元；

替換模組，根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串；

檢查模組，根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查。

本發明實施例採用的上述至少一個技術方案能夠達到以下有益效果：

業務提供方的伺服器在針對用戶進行檢查的過程中，伺服器會針對驗證碼進行字元替換的操作，相對於用戶個人而言，採用字元替換方式所產生的驗證碼並不會影響用戶獲知其中的含義，並且，本發明實施例的驗證碼中的字元並未採用諸如字形扭曲、顏色變換、添加背景等方式，使得用戶可以較為便捷且準確地識別出驗證碼，而對於電腦程式而言，經過字元替換後的驗證碼中可能包含多種類型的字元，並且不符合通常的語法，從而使得電腦程式難以依據識別演算法有效地識別出該驗證碼所表示的內容，

即可有效降低電腦程式執行非法操作的可能。

相較於現有技術中的驗證碼方式而言，本發明實施例中所提供的驗證方式，提升了驗證碼的可辨識性，使得用戶能夠直觀地獲知其表示的含義，從而能夠增加用戶辨識驗證碼的準確性，減少檢查過程的耗時，同時，增加了電腦程式對驗證碼的識別難度，也能夠有效降低電腦程式執行非法操作的可能。

【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1a及1b為現有技術中的驗證碼示意圖；

圖2a為本發明實施例提供的基於驗證碼的檢查過程所基於的架構示意圖；

圖2b為本發明實施例提供的基於驗證碼的檢查過程示意圖；

圖3為本發明實施例提供的產生字元替換驗證碼所基於的架構示意圖；

圖4a及4b為本發明實施例提供的不同檢查方式的檢查介面示意圖

圖5為本發明實施例提供的基於驗證碼的檢查裝置結構示意圖。

【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。

需要說明的是，在本發明實施例中，檢查過程可基於如圖2a所示的架構，檢查過程可由線上業務提供方後台的伺服器實現，其中，線上業務提供方包括但不限於：網站、電信運營商、資料中心等能夠提供線上業務的業務提供方。用於實現檢查過程的伺服器，具體可以是負責安全維護功能伺服器，如：線上業務提供方後台的安全中心伺服器。這裡並不構成對本發明的限定。在後續描述中，將線上系統後台的伺服器統一稱為：伺服器。

所述的用戶，可理解為使用線上業務提供方所提供的業務服務的操作者，這裡需要說明的是，在本發明實施例中的檢查情況下，合法的操作者應為自然人，而非法的操作者為電腦腳本、程式等。

以下結合附圖，詳細說明本發明各實施例提供的技術方案。

如圖2所示，示出了本發明實施中的基於驗證碼的檢查過程，該過程具體包括以下步驟：

S201：接收檢查請求。

在本發明實施例中，所述的檢查請求通常在觸發檢查後產生，實際操作中，可由用戶觸發，也可由伺服器自行根據實際應用的需要觸發。

具體地，在一種可能的情況中，用戶可以主動發送檢查請求，此時，所述的檢查請求用於觸發驗證碼的檢查過程。作為該情況中的一種方式，驗證碼的檢查過程可以應用在帳戶登錄的情況下，換言之，當用戶進入登錄介面（如：網站的帳戶登錄介面）後，便可視為用戶發出檢查請求，相應地，伺服器便會接收到用戶發送的檢查請求。

在另一種可能的情況中，伺服器可以自行按照相應的安全規則，對用戶進行身分檢查，如：按照設定的週期，伺服器主動產生驗證碼；或者，伺服器判定用戶的某些操作具有風險時，主動產生驗證碼，向用戶發起檢查，以便確定操作者不是由電腦程式所發出。當然，這裡並不構成對本發明的限定。

S202：當接收到所述檢查請求後，獲取預先產生的第一字串。

其中，所述第一字串中包含至少一個可變字元。

所述的第一字串，可理解為由數字、文字等構成且具有指示作用的標定字串。

正是考慮到在實際應用情況下，對於標定的字串較容易被電腦程式識別，從而增加了驗證過程的風險。故在本發明實施例中，第一字串中包含可變字元，該可變字元可

被替換成其他字元，以便起到干擾作用。

S203：根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串。

所述的備用字元，即可以與可變字元屬於同類別的字元，如：備用字元與可變字元均屬於中文字元、英文字元、數字字元，也可以與可變字元屬於不同的字元類別。具體來說，作為本發明實施例中的一種方式，可將漢字轉換為拼音，如：將“紅”轉換為“hong”，作為另一種方式，可將某一文字（或片語）轉換為同音字（或片語），如：將“藍色”轉換為“蘭色”。

需要說明的是，經過字元替換後的第二字串，其所要表示的含義並不會改變，也即，對應用戶而言，仍能夠獲知驗證碼所表示的含義，並可基於驗證碼執行相應的操作。

S204：根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查。

所述的驗證碼，在實際操作時，可採用圖片或文本資訊等格式展示，並用於指示用戶執行某一特定操作，這裡並不構成對本發明的限定。

正是由於第二字串是進行字元替換的字串，那麼，由第二字串所產生的驗證碼，能夠起到干擾作用，相較於現有技術中依賴字形扭曲、變色、背景等干擾的方式而言，本發明實施例中經字元替換的驗證碼所表示的含義並不會

改變，並且由於不採用過於複雜的變化的方式，既能夠使得用戶獲知驗證碼所表示的含義，也能夠使得用戶可以較為容易地進行識別，此外，由於進行了字元替換，增加了機器識別的難度。

經過前述內容，在產生了驗證碼後，便可以針對相應的操作者（即，用戶）進行檢查，以區分操作者是用戶個人還是電腦程式。

當然，作為本發明實施例中的一種可行方式，可以在相應的檢查介面（如：登錄介面）中向用戶展示驗證碼，並在用戶根據該驗證碼執行了相應的操作，根據標定檢查資訊對用戶的操作進行檢查。

透過上述步驟，業務提供方的伺服器在針對用戶進行檢查的過程中，伺服器會針對驗證碼進行字元替換的操作，相對於用戶個人而言，採用字元替換方式所產生的驗證碼並不會影響用戶獲知其中的含義，並且，本發明實施例的驗證碼中的字元並未採用諸如字形扭曲、顏色變換、添加背景等方式，使得用戶可以較為便捷且準確地識別出驗證碼，而對於電腦程式而言，經過字元替換後的驗證碼中可能包含多種類型的字元，並且不符合通常的語法，從而使得電腦程式難以依據識別演算法有效地識別出該驗證碼所表示的內容，即可有效降低電腦程式執行非法操作的可能。

相較於現有技術中的驗證碼方式而言，本發明實施例中所提供的驗證方式，提升了驗證碼的可辨識性，使得用

戶能夠直觀地獲知其表示的含義，從而能夠增加用戶辨識驗證碼的準確性，減少檢查過程的耗時，同時，增加了電腦程式對驗證碼的識別難度，也能夠有效降低電腦程式執行非法操作的可能。

需要說明的是，在本發明實施例中，針對驗證碼的字元替換，由於不改變驗證碼所表示的含義，故實質上是將驗證碼中的字元進行同音或同義替換，也即，預先建立可變字元與備用字元的對應關係，具體包括：針對任一可變字元，確定該可變字元的至少一個同音字元和/或同義字元，將確定的所述同音字元和/或同義字元作為該可變字元的備用字元，並建立與所述可變字元的對應關係。

上述內容中所述的第一字串，可認為是預先根據相應的驗證碼產生規則產生，並儲存在伺服器側的資料庫中，其架構示意圖如圖3所示。

在進行字元替換的過程，可僅將個別的可變字元進行替換，如：某驗證碼字串為漢字構成的字串“輸入兩個漢字”，假設該字串中的六個漢字均為可變字元，實際操作時，可僅將其中兩個可變字元“兩”及“漢”進行替換，假設這兩個可變字元分別對應有各自的備用字元：“倆”及“焊”，從而將可變字元替換為備用字元後的第二字串變為：“輸入倆個焊字”。

當然，也可將全部的字元進行替換，如：對於第一字串：“紅球”，假設其中兩個字元均為可變字元，各自分別對應的備用字元為拼音：“hong”以及“qiu”，則經過字元替

換後的第二字串為：“hongqiu”。

在實際應用時，如果可變字串對應不同的備用字元，那麼，也可以採用混合式的替換方式，如：將第一字串“選擇兩個紅球”，替換為“xuan擇倆個hong求”。

顯然，透過上述的替換方式，用戶個人能夠獲知驗證碼字元所表示的含義，但對於電腦程式而言，將受到較強的干擾。

在實際操作時，可基於字元替換後的第二字串，產生相應的驗證碼，根據所述第二字串產生驗證碼，具體包括：根據所述第二字串，產生指定格式的驗證碼。其中，所述指定格式包括：圖片格式、文本格式中的至少一種。

在實際應用情況下，用戶通常會根據驗證碼執行某種操作，例如：用戶根據驗證碼輸入相應的字串，又或者，用戶根據驗證碼所指示的行為，執行某種操作。而無論是用戶輸入字串或是執行某種操作，在伺服器側，都需進行檢查，為了保證檢查的準確性，故在伺服器側將確定檢查標準。可以理解地，所述的標定檢查信息，是一種檢查標準，只有用戶的操作符合該檢查標準，才可透過檢查。

作為在實際應用情況下的一種檢查方式，用戶可以根據檢查介面中所展示的驗證碼輸入相應的字串，在此方式下，標定檢查資訊就是第一字串，對所述檢查請求所對應的用戶進行檢查，具體包括：在對用戶進行檢查的介面上，產生輸入區域，獲取用戶在所述輸入區域內根據所述驗證碼所輸入的待檢查字串，根據所述第一字串，對所述

待檢查字串進行檢查。

也即，如圖4a所示，示出了該方式下的檢查介面，可見，該檢查介面中包含驗證碼和相應的輸入區域，用戶根據驗證碼在該輸入區域中輸入相應的字串以進行檢查，當然，在圖4a中，用戶根據驗證碼“hong色”（該驗證碼中為第二字串），在輸入區中輸入漢字片語“紅色”後（假設第一字串：紅色），才可透過檢查。

而作為在實際應用情況下的另一種檢查方式，用戶可以根據檢查介面中所展示的驗證碼執行相應的檢查操作，在此方式下，所述標定檢查資訊包括：預設的標準操作資訊，對所述檢查請求所對應的用戶進行檢查，具體包括：在對用戶進行檢查的介面上，產生可操作的驗證碼展示區，獲取所述用戶在驗證碼展示區內，根據所述驗證碼所執行的待檢查操作所對應的待檢查操作資訊，根據所述標定操作資訊，對所述待檢查操作資訊進行檢查。

如圖4b所示，示出了該方式下的檢查介面，可見，該檢查介面中包含可操作且攜帶驗證碼的驗證碼展示區，用戶可以根據驗證碼所指示的行為，在該驗證碼展示區發出相應的待檢查操作，在圖4b中，假設標準操作資訊為操作控制項“2”和“4”被點擊，那麼，用戶根據驗證碼“點擊下圖中的ou數”，針對驗證碼展示區內的操作控制項“2”和“4”進行點擊後，可透過檢查。

當然，上述兩種方式僅是為了說明本發明實施例中的檢查方法，並不構成對本發明的限定。

以上為本發明實施例提供的檢查方法，基於同樣的思路，本發明實施例還提供一種基於驗證碼的檢查裝置。

如圖5所示，所述的檢查裝置，設置於業務提供方的伺服器側，該裝置包括：

接收模組501，接收檢查請求；

獲取模組502，當接收到所述檢查請求後，獲取預先產生的第一字串；其中，所述第一字串中包含至少一個可變字元；

替換模組503，根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串；

檢查模組504，根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查。

所述裝置還包括：建立模組505，針對任一可變字元，確定該可變字元的至少一個同音字元和/或同義字元，將確定的所述同音字元和/或同義字元作為該可變字元的備用字元，並建立與所述可變字元的對應關係。

所述檢查模組504，根據所述第二字串，產生指定格式的驗證碼。其中，所述指定格式包括：圖片格式、文本格式中的至少一種。

所述檢查模組504，在對用戶進行檢查的介面上，產生輸入區域，獲取用戶在所述輸入區域內根據所述驗證碼所輸入的待檢查字串，根據所述第一字串，對所述待檢查字串進行檢查。

所述檢查模組504，在對用戶進行檢查的介面上，產生可操作的驗證碼展示區，獲取所述用戶在驗證碼展示區內，根據所述驗證碼所執行的待檢查操作所對應的待檢查操作資訊，根據預設的標定操作資訊，對所述待檢查操作資訊進行檢查。

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，對二極體、電晶體、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。設計人員幾乎都透過將改進的方法流程程式設計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，可程式設計邏輯器件（Programmable Logic Device, PLD）（例如現場可程式設計閘陣列（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程式設計來確定。由設計人員自行程式設計來把一個數位系統“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。而且，如今，取代手工地製作積體電路晶片，這種程式設計也多半改用“邏輯編譯器（logic compiler）”軟體來實現，它與程式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程式設計語言來撰寫，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Verilog。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程式設計並程式設計到積體電路中，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）處理器執行的電腦可讀程式碼（例如軟體或固件）的電腦可讀媒體、邏輯閘、開關、專用積體電路（Application Specific Integrated Circuit, ASIC）、可程式設計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，記憶體控制器還可以被實現為記憶體的控制邏輯的一部分。本領域技術人員也知道，除了以純電腦可讀程式碼方式實現控制器以外，完全可以透過將方法步驟進行邏輯程式設計來使得控制器以邏輯閘、開關、專用積

體電路、可程式設計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，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦。具體的，電腦例如可以為個人電腦、膝上型電腦、蜂巢式電話、相機電話、智慧型電話、個人數位助理、媒體播放機、導航設備、電子郵件設備、遊戲控制台、平板電腦、可穿戴設備或者這些設備中的任何設備的組合。

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媒體（包括但不限於磁碟記憶體、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／或方塊圖來描述的。應理解可由電腦程式指令實現流程圖和／或方塊圖中的每一流程和／或方塊、以及流程圖和／或方塊圖中的流程和／或方塊的結合。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程式設計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程式設計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／或方塊圖一個方塊或多個方塊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程式設計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／或方塊圖一個方塊或多個方塊中指定的功能。

這些電腦程式指令也可裝載到電腦或其他可程式設計資料處理設備上，使得在電腦或其他可程式設計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程式設計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／或方塊圖一個方塊或多個方塊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、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體(RAM)和/或非易失性記憶體等形式，如唯

讀記憶體(ROM)或快閃記憶體(flash RAM)。記憶體是電腦可讀媒體的示例。

電腦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。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體(PRAM)、靜態隨機存取記憶體(SRAM)、動態隨機存取記憶體(DRAM)、其他類型的隨機存取記憶體(RAM)、唯讀記憶體(ROM)、電可擦除可程式設計唯讀記憶體(EEPROM)、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體(CD-ROM)、數位多功能光碟(DVD)或其他光學儲存、磁盒式磁帶，磁帶磁磁片儲存或其他磁性存放裝置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，電腦可讀媒體不包括暫態式電腦可讀媒體(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媒體（包括但不限於磁碟記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

本發明可以在由電腦執行的電腦可執行指令的一般上下文中描述，例如程式模組。一般地，程式模組包括執行特定事務或實現特定抽象資料類型的常式、程式、物件、元件、資料結構等等。也可以在分散式運算環境中實踐本發明，在這些分散式運算環境中，由透過通信網路而被連接的遠端處理設備來執行事務。在分散式運算環境中，程式模組可以位於包括存放裝置在內的本地和遠端電腦儲存媒體中。

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照即可，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的

範圍之內。

【符號說明】

S201、S202、S203、S204：方法步驟

501：接收模組

502：獲取模組

503：替換模組

504：檢查模組

505：建立模組

第 106132402 號　　民國 110 年 9 月 17 日修正

【發明申請專利範圍】

【第1項】

一種基於驗證碼的檢查方法，其特徵在於，該方法包括：

伺服器接收檢查請求；

當該伺服器接收到該檢查請求後，獲取預先產生的第一字串，其中，該第一字串中包含至少一個可變字元，其中，該第一字串是執行一個或多個操作的第一指示；

該伺服器根據預先建立的可變字元與備用字元的對應關係，將該第一字串中的一個或多個可變字元中的至少一個替換為至少一個備用字元，得到第二字串，其中，該第一字串中的一個或多個可變字元中的至少一個的替換可變字元與該至少一個備用字元的對應備用字元為同音字元或同義字元，第二字串為執行一個或多個操作的第二指示；

該伺服器根據該第二字串產生指定格式的驗證碼，對該檢查請求所對應的用戶進行檢查，其中，該指定格式包括圖片格式、文本格式中的至少一種，經過字元替換後產生的該驗證碼所表示的含義不會改變，使得該用戶能夠獲知該驗證碼所表示的含義；以及

該伺服器展示該驗證碼和與該驗證碼相對應的輸入區域，其中，該輸入區域包括多個可選項目，並且該驗證碼指示用戶從多個可選項目中選擇一個或多個可選項目。

【第2項】

如申請專利範圍第1項所述的方法，其中，預先建立

可變字元與備用字元的對應關係，具體包括：

該伺服器針對任一可變字元，確定該可變字元的至少一個同音字元和/或同義字元；以及

該伺服器將確定的該同音字元和/或同義字元作為該可變字元的備用字元，並建立與該可變字元的對應關係。

【第3項】

如申請專利範圍第1項所述的方法，其中，對該檢查請求所對應的用戶進行檢查，具體包括：

該伺服器在對用戶進行檢查的介面上，產生輸入區域；

該伺服器獲取用戶在該輸入區域內根據該驗證碼所輸入的待檢查字串；以及

該伺服器根據該第一字串，對該待檢查字串進行檢查。

【第4項】

如申請專利範圍第1項所述的方法，其中，對該檢查請求所對應的用戶進行檢查，具體包括：

該伺服器在對用戶進行檢查的介面上，產生可操作的驗證碼展示區；

該伺服器獲取該用戶在驗證碼展示區內，根據該驗證碼所執行的待檢查操作所對應的待檢查操作資訊；以及

該伺服器根據預設的標定操作資訊，對該待檢查操作資訊進行檢查。

【第5項】

一種基於驗證碼的檢查裝置，其特徵在於，該裝置包括：

接收模組，接收檢查請求；

獲取模組，當接收到該檢查請求後，獲取預先產生的第一字串，其中，該第一字串中包含至少一個可變字元，其中，該第一字串是執行一個或多個操作的第一指示；

替換模組，根據預先建立的可變字元與備用字元的對應關係，將該第一字串中的一個或多個可變字元中的至少一個替換為至少一個備用字元，得到第二字串，其中，該第一字串中的一個或多個可變字元中的至少一個的替換可變字元與該至少一個備用字元的對應備用字元為同音字元或同義字元，第二字串為執行一個或多個操作的第二指示；以及

檢查模組，根據該第二字串產生指定格式的驗證碼，對該檢查請求所對應的用戶進行檢查，其中，該指定格式包括圖片格式、文本格式中的至少一種，經過字元替換後產生的該驗證碼所表示的含義不會改變，使得該用戶能夠獲知該驗證碼所表示的含義；以及

該伺服器展示該驗證碼和與該驗證碼相對應的輸入區域，其中，該輸入區域包括多個可選項目，並且該驗證碼指示用戶從多個可選項目中選擇一個或多個可選項目。

【第6項】

如申請專利範圍第5項所述的裝置，其中，該裝置還包括：建立模組，針對任一可變字元，確定該可變字元的

至少一個同音字元和/或同義字元，將確定的該同音字元和/或同義字元作為該可變字元的備用字元，並建立與該可變字元的對應關係。

【第7項】

如申請專利範圍第5項所述的裝置，其中，該檢查模組，在對用戶進行檢查的介面上，產生輸入區域，獲取用戶在該輸入區域內根據該驗證碼所輸入的待檢查字串，根據該第一字串，對該待檢查字串進行檢查。

【第8項】

如申請專利範圍第5項所述的裝置，其中，該檢查模組，在對用戶進行檢查的介面上，產生可操作的驗證碼展示區，獲取該用戶在驗證碼展示區內，根據該驗證碼所執行的待檢查操作所對應的待檢查操作資訊，根據預設的標定操作資訊，對該待檢查操作資訊進行檢查。

【發明圖式】

圖 1a

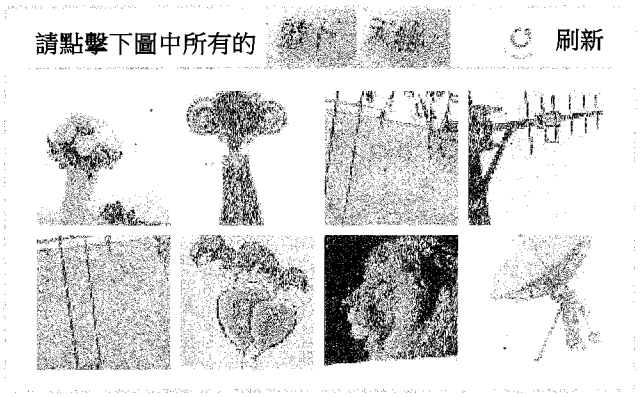

圖 1b

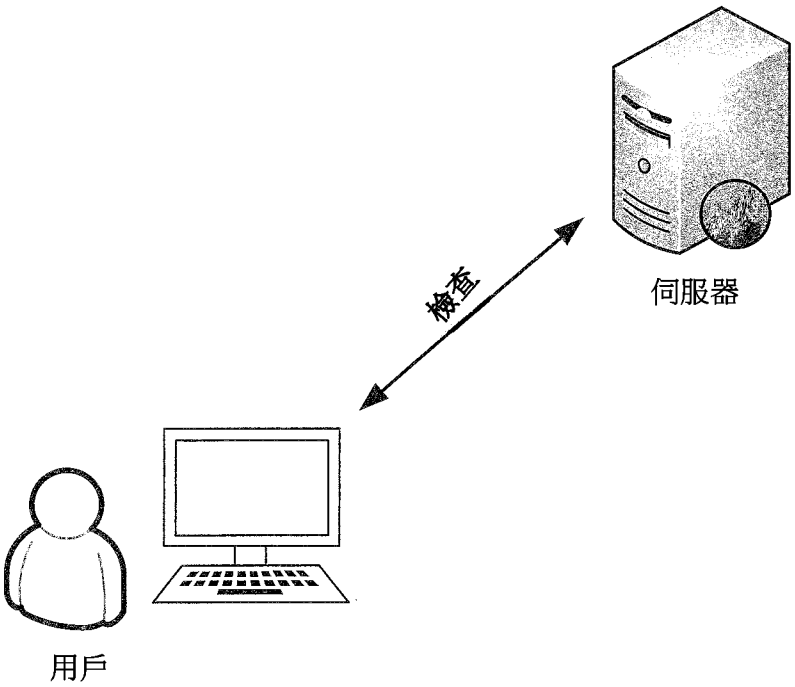

圖 2a

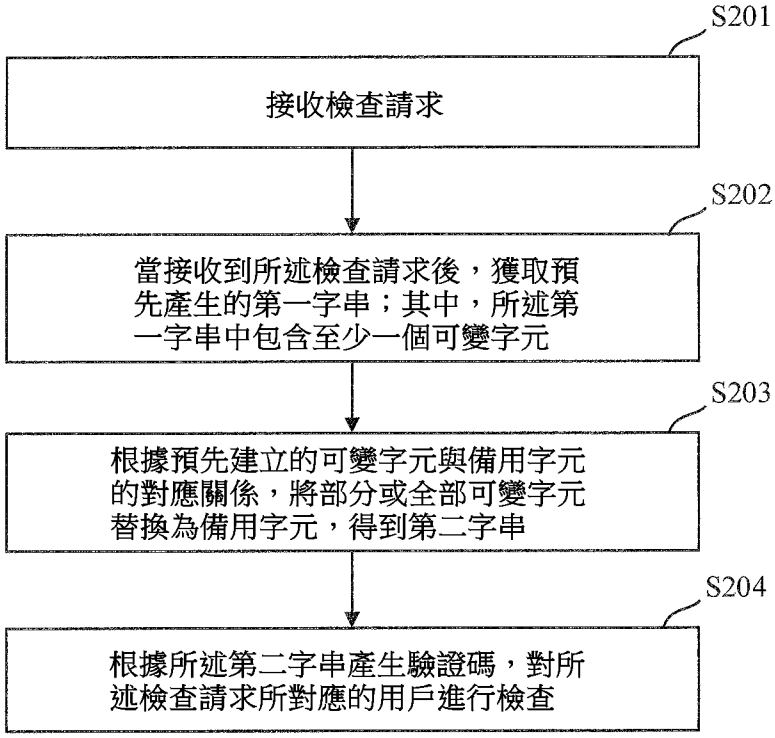
S201
接收檢查請求
S202
當接收到所述檢查請求後，獲取預先產生的第一字串；其中，所述第一字串中包含至少一個可變字元
S203
根據預先建立的可變字元與備用字元的對應關係，將部分或全部可變字元替換為備用字元，得到第二字串
S204
根據所述第二字串產生驗證碼，對所述檢查請求所對應的用戶進行檢查

圖 2b

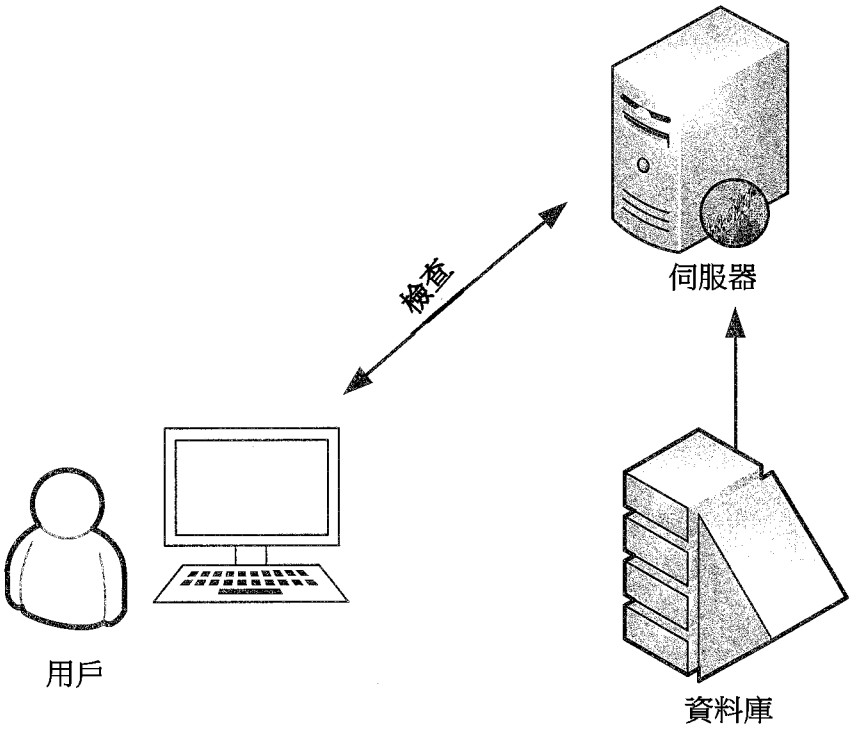
檢查
伺服器
用戶
資料庫

圖 3

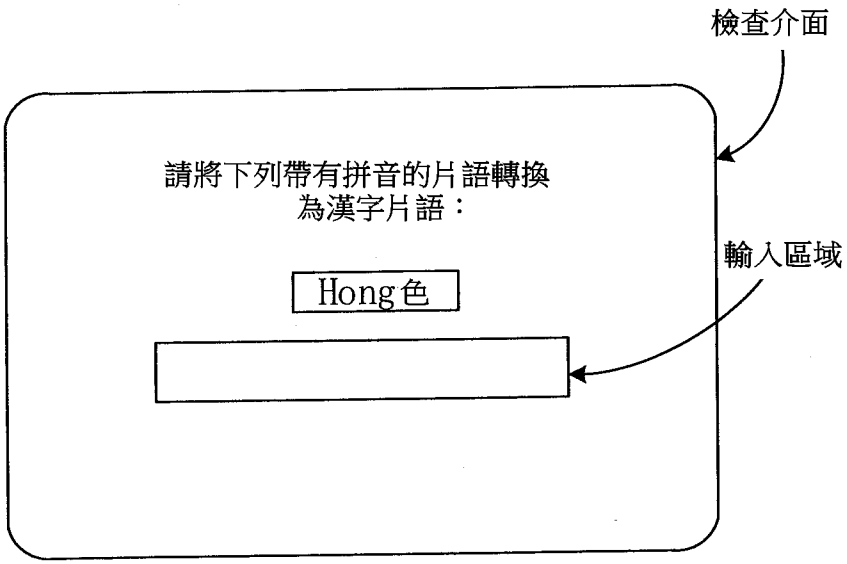
檢查介面
請將下列帶有拼音的片語轉換
為漢字片語：
Hong色
輸入區域

圖 4a

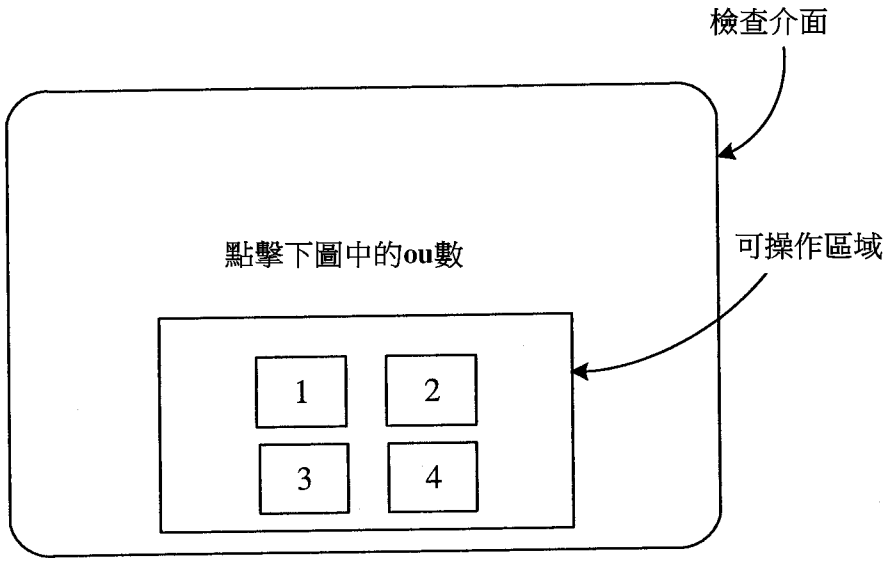
檢查介面
點擊下圖中的ou數
可操作區域
1
2
3
4

圖 4b

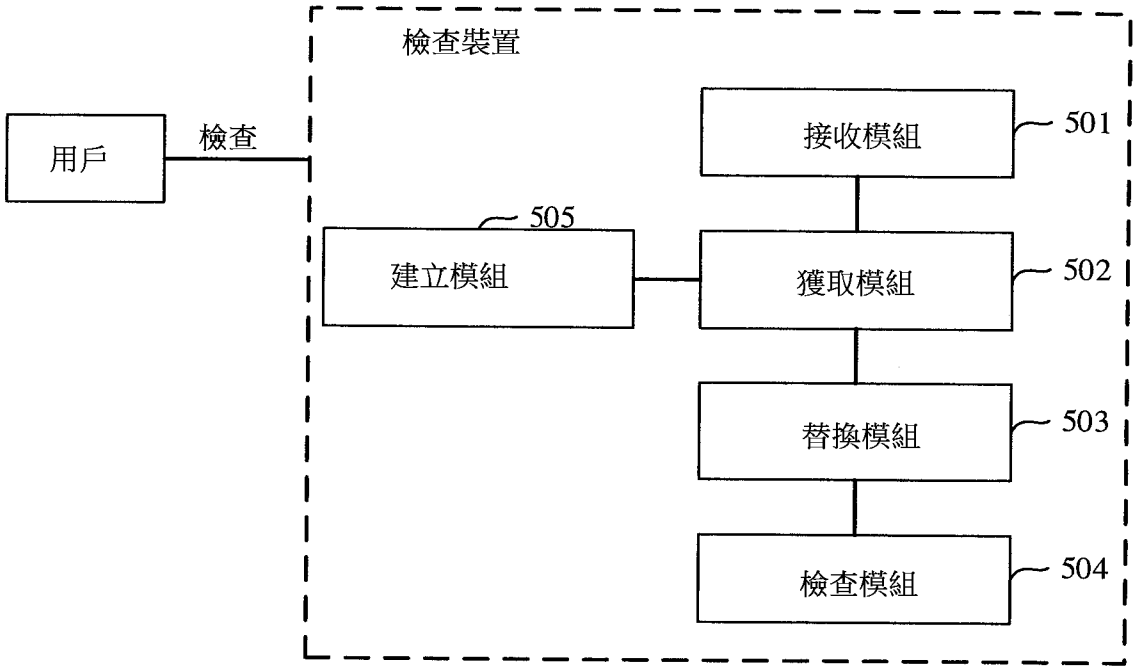

圖 5