I640890

(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 I640890 B**

(45)公告日： 中華民國 107 (2018) 年 11 月 11 日

(21)申請案號：103132984 (22)申請日： 中華民國 103 (2014) 年 09 月 24 日

(51)Int. Cl.： *G06F21/46 (2013.01)* *G06F21/31 (2013.01)*

(30)優先權：2014/04/16 中國大陸 201410153728.8

(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：章文 (CN)

(74)代理人：林志剛

(56)參考文獻：

TW	201131490A	CN	103370688A
US	20050198537A1	US	20130036459A1
US	20140068731A1		

審查人員：吳家豪

申請專利範圍項數：8 項 圖式數：5 共 25 頁

(54)名稱

檢測弱密碼的方法和裝置

(57)摘要

本發明提供一種檢測弱密碼的方法和裝置，該方法包括：接收待測密碼；獲取所述待測密碼的用戶的身份資訊集合，所述身份資訊集合中包含所述用戶及其相關用戶的多個身份資訊；檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊；如果所述身份資訊集合中存在與所述待測密碼相關的身份資訊，則確定所述待測密碼是弱密碼。採用本發明的技術方案，能夠檢測待測密碼是否是用戶利用自己的身份資訊或者與自己聯繫密切的用戶的身份資訊設置的，進而判斷待測密碼是否容易破解，進一步提高用戶密碼的安全性。

指定代表圖：

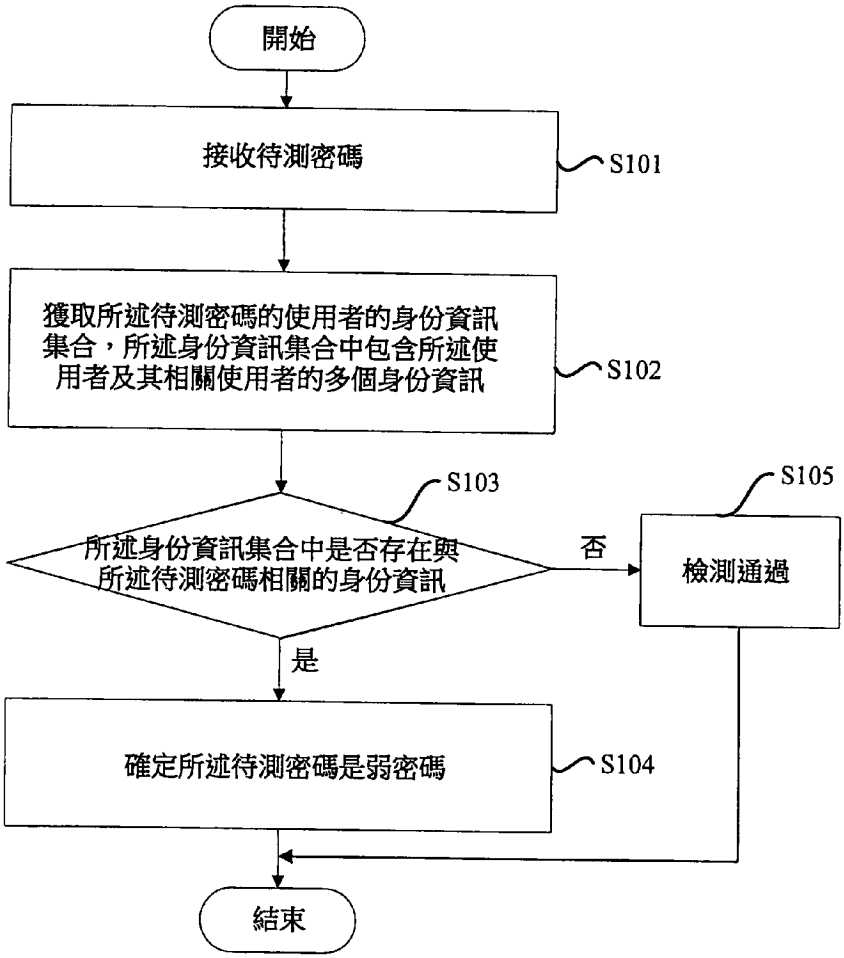
開始
接收待測密碼
S101
獲取所述待測密碼的使用者的身份資訊集合，所述身份資訊集合中包含所述使用者及其相關使用者的多個身份資訊
S102
S103
所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊
否
S105
檢測通過
是
確定所述待測密碼是弱密碼
S104
結束

圖 1

圖式

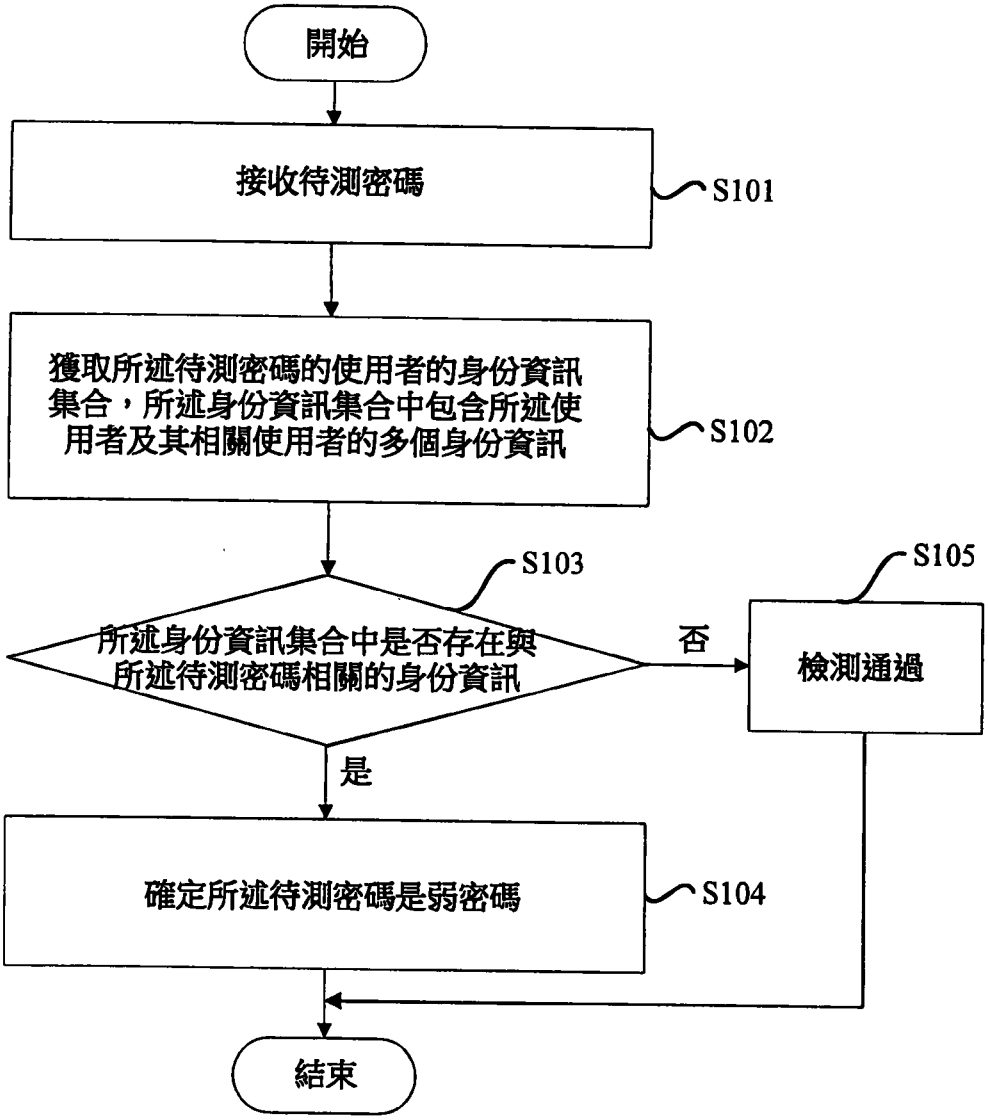
開始
接收待測密碼
S101
獲取所述待測密碼的使用者的身份資訊集合，所述身份資訊集合中包含所述使用者及其相關使用者的多個身份資訊
S102
S103
所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊
否
S105
檢測通過
是
確定所述待測密碼是弱密碼
S104
結束

圖 1

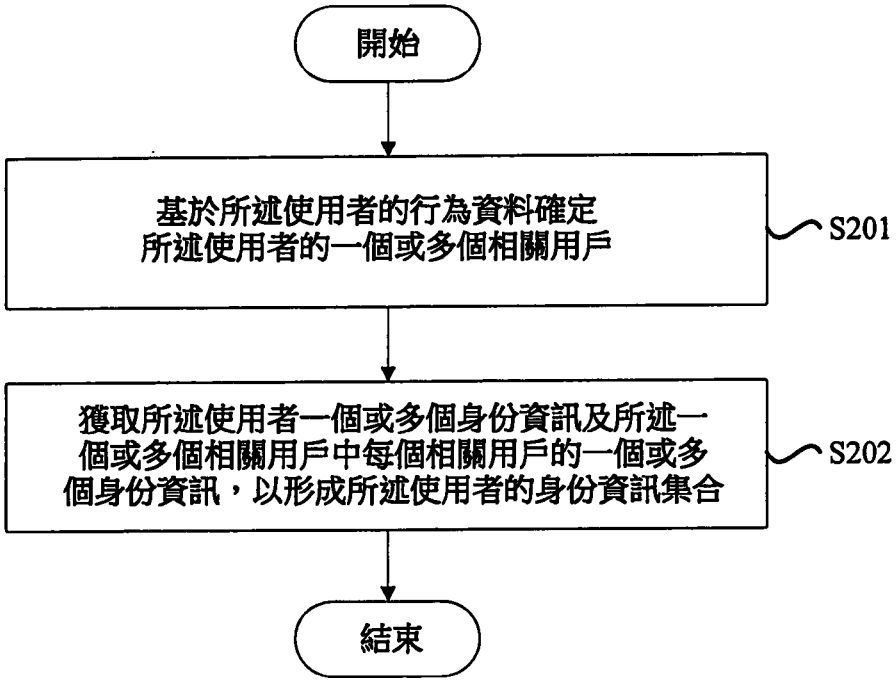
開始
基於所述使用者的行為資料確定
所述使用者的一個或多個相關用戶
S201
獲取所述使用者一個或多個身份資訊及所述一
個或多個相關用戶中每個相關用戶的一個或多
個身份資訊，以形成所述使用者的身份資訊集合
S202
結束

圖 2

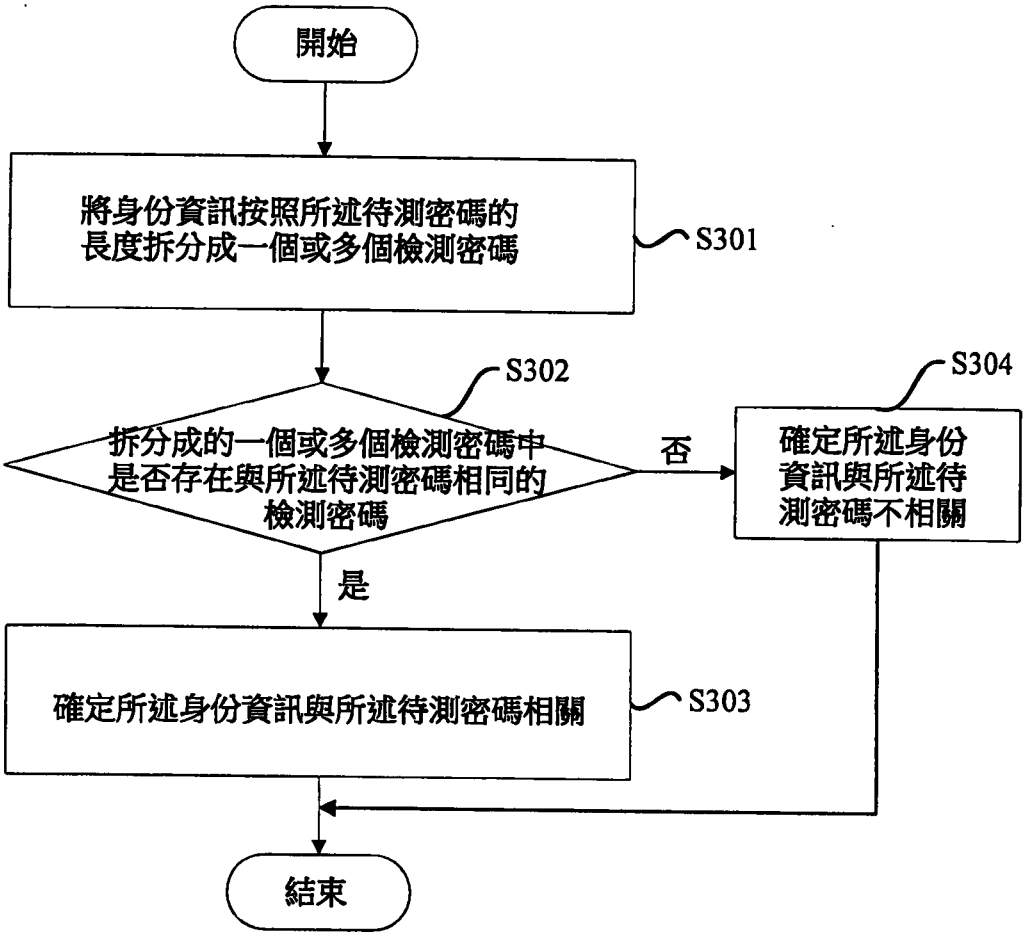
開始
將身份資訊按照所述待測密碼的長度拆分成一個或多個檢測密碼
S301
S302
拆分成的一個或多個檢測密碼中是否存在與所述待測密碼相同的檢測密碼
否
S304
確定所述身份資訊與所述待測密碼不相關
是
確定所述身份資訊與所述待測密碼相關
S303
結束

圖 3

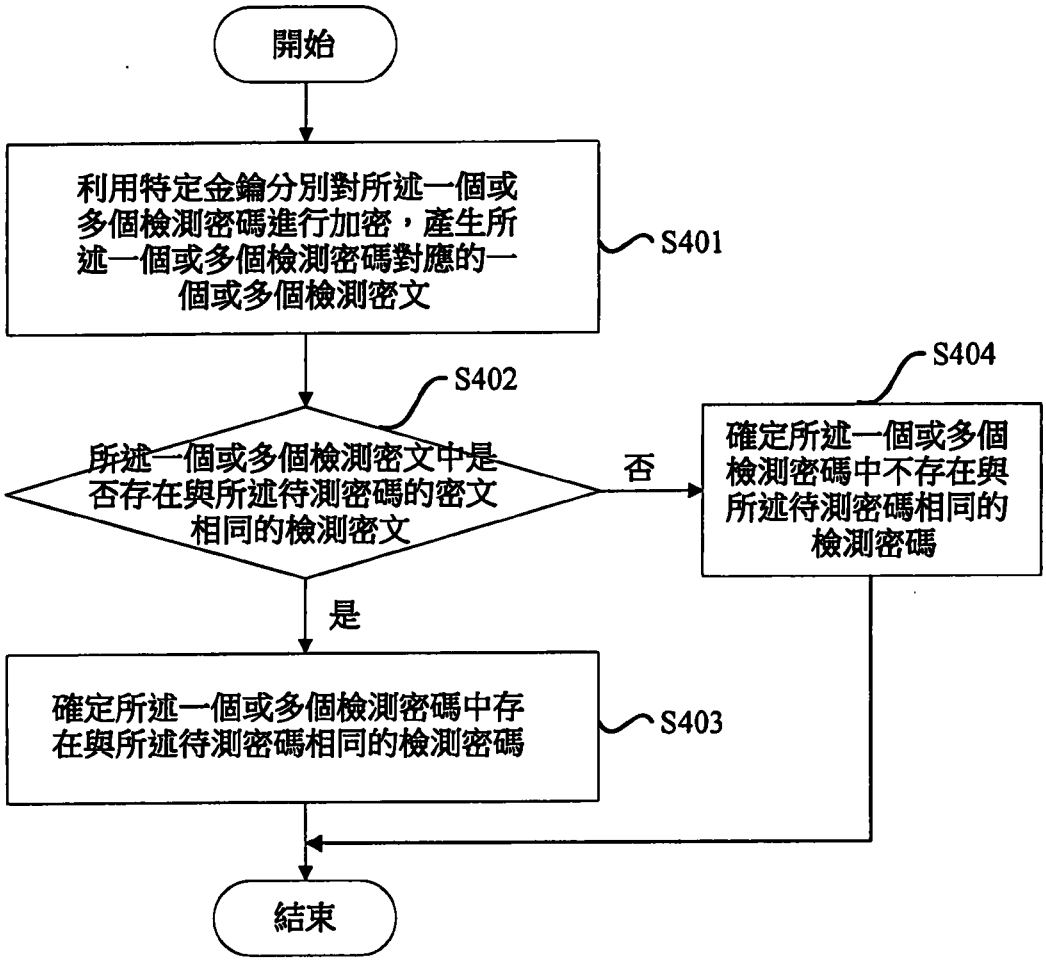
開始
利用特定金鑰分別對所述一個或多個檢測密碼進行加密，產生所述一個或多個檢測密碼對應的一個或多個檢測密文
S401
S402
所述一個或多個檢測密文中是否存在與所述待測密碼的密文相同的檢測密文
否
S404
確定所述一個或多個檢測密碼中不存在與所述待測密碼相同的檢測密碼
是
確定所述一個或多個檢測密碼中存在與所述待測密碼相同的檢測密碼
S403
結束

圖 4

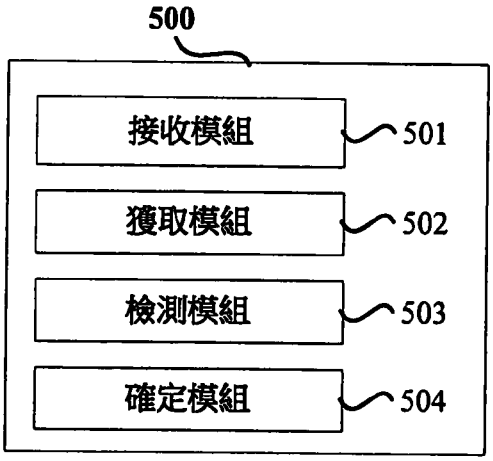

圖 5

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)

檢測弱密碼的方法和裝置

【技術領域】

本發明涉及網際網路技術領域，尤其涉及一種檢測弱密碼的方法和裝置。

【先前技術】

在目前網際網路環境中，用戶的身份相關資訊不再成為隱私資訊，嚴重影響用戶的資料和密碼安全，一些用戶在設置密碼時為了方便記憶，使用過於簡單的密碼，或者利用與自己或親友相關的資訊設置密碼，很容易被破解。

現有常見的檢測用戶弱密碼的方法主要包括：通過常用弱密碼字典，判斷用戶設置的密碼是否過於簡單；或者根據用戶的身份相關資訊，如身份證號、手機號、銀行卡號等，判斷用戶設置的密碼是否與自己身份資訊相關。

現有的用戶弱密碼檢測技術只能基於常用弱密碼和用戶自己的身份相關資訊進行檢測，然而，有些用戶常常利用與自己關係親密的人的身份資訊設置密碼，這種情況下設置的弱密碼通過現有技術是無法檢測的，無法進一步提高用戶密碼的安全性。

【發明內容】

本發明的主要目的在於提供一種檢測弱密碼的方法和裝置，以解決現有技術存在的無法檢測出用戶利用與自己相關的其他用戶的身份資訊設置的密碼的問題，其中：

本發明提供了一種檢測弱密碼的方法，包括：接收待測密碼；獲取所述待測密碼的用戶的身份資訊集合，所述身份資訊集合中包含所述用戶及其相關用戶的多個身份資訊；檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊；如果所述身份資訊集合中存在與所述待測密碼相關的身份資訊，則確定所述待測密碼是弱密碼。

本發明的另一方面提供一種檢測弱密碼的裝置，包括：接收模組，用於接收待測密碼；獲取模組，用於獲取所述待測密碼的用戶的身份資訊集合，所述身份資訊集合中包含所述用戶及其相關用戶的多個身份資訊；檢測模組，用於檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊；確定模組，用於如果所述身份資訊集合中存在與所述待測密碼相關的身份資訊，則確定所述待測密碼是弱密碼。

與現有技術相比，根據本發明的技術方案，能夠檢測待測密碼是否是用戶利用自己的身份資訊或者與自己聯繫密切的用戶的身份資訊設置的，進而判斷待測密碼是否容易破解，進一步提高了用戶密碼的安全性。

【圖式簡單說明】

此處所說明的圖式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。在圖式中：

圖 1 是本發明實施例的檢測弱密碼的方法的流程圖；

圖 2 是根據本發明一個實施例的獲取所述待測密碼的用戶的身份資訊集合的步驟的流程圖；

圖 3 是根據本發明一個實施例的檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊的步驟的流程圖；

圖 4 是根據本發明一個實施例的判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與所述待測密碼相同的檢測密碼的步驟的流程圖；以及

圖 5 是本發明實施例的檢測弱密碼的裝置的流程圖。

【實施方式】

本發明的主要思想在於，基於用戶的行為，確定與所述用戶聯繫密切的一個或多個相關用戶，獲取所述用戶及其相關用戶的多個身份資訊，並根據所述多個身份資訊判斷所述用戶所設置的密碼是否與所述多個身份資訊相關，從而確定所述待測密碼是否為弱密碼。

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圖式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，本領域中具有通常知識者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。

根據本發明的實施例，提供了一種檢測弱密碼的方法。

參考圖 1，圖 1 是本發明實施例的一種檢測弱密碼的方法的流程圖。

在步驟 S101 處，接收待測密碼。

所述待測密碼可以為用戶登錄用戶端應用、網頁應用等應用時的登錄密碼、用戶使用用戶端應用或網頁應用進行特定操作（該特定操作基於服務端提供的服務）的驗證密碼等，如，進行支付交易時的支付密碼。應當理解，待測密碼不限於此，而是可以是任何需要進行檢測的密碼。

在步驟 S102 處，獲取所述待測密碼的用戶的身份資訊集合，所述身份資訊集合中包含所述用戶及其相關用戶的多個身份資訊。

為了更清楚地解釋該步驟，參考圖 2 來描述該步驟的一種可選的具體實施。

如圖 2 所示，圖 2 是根據本發明的一個實施例的獲取所述待測密碼的用戶的身份資訊集合的步驟的流程圖。

在步驟 S201 處，基於所述用戶的行為資料，確定所述用戶的一個或多個相關用戶。

其中，所述用戶的一個或多個相關用戶可以為與所述

用戶聯繫密切的一個或多個用戶，與該用戶聯繫密切的用戶例如可以包括該用戶的親戚、好友等。所述用戶的行為資料可以包括：用戶的交互行為的行為資料，如，與所述用戶有交易行為（例如，轉帳，包括給其他用戶的轉帳或接收的其他用戶的轉帳）的用戶，用戶的瀏覽行為的行為資料，如，該用戶瀏覽過的用戶。

具體地，可以統計該用戶的行為資料並進行分析，得到與所述用戶聯繫最密切的一個或多個用戶作為該用戶的相關用戶。該一個或多個相關用戶的數量可以根據具體情況確定，例如，可以通過統計與該用戶進行過交互的用戶，將與該用戶交互最頻繁的預定數量的用戶（TopN）作為該用戶的相關用戶，或者可以將與該用戶交互次數超過預定次數的一個或多個用戶作為該用戶的相關用戶。

在步驟 S202 處，獲取所述用戶一個或多個身份資訊及所述一個或多個相關用戶中每個相關用戶的一個或多個身份資訊，以形成所述用戶的身份資訊集合。其中，每個身份資訊可以由多個字元（例如，數位、字母）構成，身份資訊可以包括：姓名、身份證號、手機號、銀行帳號/卡號等資訊。即，可以獲取該用戶的上述身份資訊中的一個或多個身份資訊以及該用戶的每個相關用戶的上述身份資訊中的一個或多個身份資訊，以形成該用戶的身份資訊集合。

返回圖 1，在步驟 S103 處，檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊。即，檢測該

待測密碼是否是用戶利用與自己的身份資訊或與自己聯繫密切的用戶的身份資訊設置的。

為了更清楚地解釋該步驟，我們參考圖 3 來描述該步驟的一種可選的具體實施。

可參考圖 3，圖 3 示出了根據本發明一個實施例的檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊的步驟（步驟 S103）的流程圖。需說明的是，圖 3 所示為分別針對每個身份資訊判斷該身份資訊是否與待測密碼相關的流程圖。

在步驟 S301 處，將所述身份資訊集合中的每個身份資訊按照所述待測密碼的長度拆分成一個或多個檢測密碼。

根據本發明的一個實施例，可以從系統先獲取該待測密碼的長度，再根據該待測密碼的長度，將每個身份資訊拆分成與該待測密碼長度相同的一個或多個檢測密碼。每個身份資訊所拆分成的一個或多個檢測密碼用於在下一個步驟中與該待測密碼進行比較，從而判斷該身份資訊是否與該密碼相關。

具體地，對於任意一個身份資訊，可以按該身份資訊中字元（如，數位、字母）的排列順序將其拆分為（L-M+1）個長度為 M 的檢測密碼。其中，L 為身份資訊的長度，M 為待測密碼的長度。例如，假設待測密碼的長度為 6，對於身份資訊“123456789”，可以將其拆分成“123456”、“234567”、“345678”、“456789”4 個

檢測密碼。

在步驟 S302 處，判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與所述待測密碼相同的檢測密碼。

參考圖 4，圖 4 示出了根據本發明一個可選實施例的判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與所述待測密碼相同的檢測密碼的步驟（步驟 S302）的流程圖。

如圖 4 所示，針對每個身份資訊拆分成的一個或多個檢測密碼，在步驟 S401 處，利用特定金鑰分別對所述一個或多個檢測密碼進行加密，產生所述一個或多個檢測密碼對應的一個或多個檢測密文。

具體地，在用戶輸入密碼（例如，用戶設置密碼時進行的輸入或用戶使用密碼進行相關驗證時的輸入）時，（系統）為保證用戶的密碼安全，可以利用特定金鑰對用戶輸入的密碼進行加密，產生該密碼的密文，以防止用戶的密碼被竊取。因此，（伺服器端）所接收到的用戶輸入的密碼或者獲取到的保存（在伺服器端）的用戶預先設置的密碼是利用該特定金鑰加密過的密文。因此，接收該待測密碼時，實際上接收到的是利用該特定金鑰對該待測密碼進行加密後產生的密文。所以，可以獲取該特定金鑰，並利用該特定金鑰分別對該一個或多個檢測密碼進行加密，產生與每個檢測密碼對應的一個或多個檢測密文，以便將所述一個或多個檢測密文與待測密碼的密文進行比

較，確定是否存在與該待測密碼相同的檢測密文。

在步驟 S402 處，判斷所述一個或多個檢測密文中是否存在與所述待測密碼的密文相同的檢測密文。其中，所述待測密碼的密文是利用所述特定金鑰對所述待測密碼進行加密產生的。

具體地，可以將該一個或多個檢測密文與該待測密碼的密文進行比較，逐個判斷每個檢測密文是否與該待測密碼的密文相同。

在步驟 S403 處，如果所述一個或多個檢測密文中存在與所述待測密碼的密文相同的檢測密文，則確定所述一個或多個檢測密碼中存在與所述待測密碼相同的檢測密碼。

由於該一個或多個檢測密文與該待測密碼是利用相同的金鑰（特定金鑰）加密產生的，因此，如果檢測到任意一個檢測密文與該待測密碼的密文相同，則可以確定該檢測密文對應的檢測密碼（即，產生該檢測密文的檢測密碼）與該待測密碼相同，並且還可以確定所述一個或多個檢測密碼中存在與所述待測密碼相同的檢測密碼。如果所述一個或多個檢測密文中不存在任何一個與所述待測密碼的密文相同的檢測密文，則可以在步驟 S404 處，確定所述一個或多個檢測密碼中不存在與所述待測密碼相同的檢測密碼。

回到圖 3，在步驟 S303 處，對所述身份資訊集合中的每個身份資訊分別進行上述的步驟 S401~S404 之後，如

果任意一個身份資訊拆分成的一個或多個檢測密碼中存在與所述待測密碼相同的檢測密碼，則確定所述身份資訊與所述待測密碼相關，即，可以確定所述身份資訊集合中存在與所述待測密碼相關的身份資訊。如果該身份資訊拆分成的一個或多個檢測密碼中不存在與所述待測密碼相同的檢測密碼，則可以在步驟 S304 處，確定所述身份資訊與所述待測密碼不相關。

如果任何一個身份資訊拆分成的一個或多個檢測密碼中都不存在與所述待測密碼相同的檢測密碼，則可以確定所述身份資訊集合中不存在與所述待測密碼相關的身份資訊。

以上借助圖 3 和圖 4 更詳細地描述了步驟 S103 的一種優選的詳細實施，下面返回圖 1 繼續描述。在步驟 S104 處，如果所述身份資訊集合中存在與所述待測密碼相關的身份資訊，則確定所述待測密碼是弱密碼。

具體而言，對該身份資訊集合中包含的多個身份資訊逐個進行步驟 S301~S304，分別判斷每個身份資訊是否與該待測密碼相關，如果所述身份資訊集合中存在任意一個與所述待測密碼相關的身份資訊，則說明用戶是利用該身份資訊設置的該待測密碼，則該待測密碼可能容易被破解，是弱密碼。

如果所述身份資訊集合中不存在與所述待測密碼相關的身份資訊，則說明該待測密碼與該身份資訊集合中的各個身份資訊都不相關，即，用戶不是利用該身份資訊集合

中的任何一個身份資訊設置的該待測密碼，則可以在步驟 S105 處，確定檢測通過。也即是說待測密碼不是弱密碼，檢測通過。

本發明的技術方案可以用於檢測用戶的密碼是否是利用自己的身份資訊或與自己聯繫密切的相關用戶的身份資訊設置的，可以用於利用弱密碼字典進行的弱密碼檢測之前，也可以用於利用弱密碼字典進行的弱密碼檢測之後。

本發明還提供了一種檢測弱密碼的裝置。

圖 5 示意性地示出了根據本發明一個實施例的檢測弱密碼的裝置的結構方塊圖。

根據本發明的一個實施例，該裝置 500 包括：接收模組 501、獲取模組 502、檢測模組 503 和確定模組 504。

其中，接收模組 501 可以用於接收待測密碼。

獲取模組 502 可以用於獲取所述待測密碼的用戶的身份資訊集合，所述身份資訊集合中包含所述用戶及其相關用戶的多個身份資訊。

檢測模組 503 可以用於檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊。

確定模組 504 可以用於如果所述身份資訊集合存在與所述待測密碼相關的身份資訊，則確定所述待測密碼是弱密碼。

根據本發明的實施例，獲取模組 502 可以包括：相關用戶確定模組和身份資訊獲取模組。

其中，相關用戶確定模組可以用於基於所述用戶的行

為資料確定所述用戶的一個或多個相關用戶。

身份資訊獲取模組可以用於獲取所述用戶的一個或多個身份資訊及所述一個或多個相關用戶中每個相關用戶的一個或多個身份資訊，以形成所述用戶的身份資訊集合。

根據本發明的實施例，檢測模組 503 可以包括：拆分模組、判斷模組以及第一確定模組。

拆分模組可以用於將所述身份資訊集合中的每個身份資訊按照所述待測密碼的長度分別拆分成一個或多個檢測密碼。

判斷模組可以用於判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與所述待測密碼相同的檢測密碼。

第一確定模組可以用於如果任意一個身份資訊拆分成的一個或多個檢測密碼中存在與所述待測密碼相同的檢測密碼，則確定所述身份資訊與所述待測密碼相關。

根據本發明的實施例，判斷模組可以包括：產生子模組、判斷子模組以及確定子模組。

其中，產生子模組可以用於利用特定金鑰分別對所述一個或多個檢測密碼進行加密，產生所述一個或多個檢測密碼對應的一個或多個檢測密文。

判斷子模組可以用於判斷所述一個或多個檢測密文中是否與所述待測密碼的密文相同的檢測密文，其中，所述待測密碼的密文是利用所述特定金鑰對所述待測密碼進行加密產生的。

確定子模組可以用於如果所述一個或多個檢測密文中存在與所述待測密碼的密文相同的檢測密文，則確定所述一個或多個檢測密碼中存在與所述待測密碼相同的檢測密碼。

由於本實施例的裝置所實現的功能基本相應於前述圖 1 至圖 4 所示的方法實施例，故本實施例的描述中未詳盡之處，可以參見前述實施例中的相關說明，在此不做贅述。

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介質中的非永久性記憶體，隨機存取記憶體 (RAM) 和/或非揮發性記憶體等形式，如唯讀記憶體 (ROM) 或快閃記憶體(flash RAM)。記憶體是電腦可讀介質的示例。

電腦可讀介質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。電腦的儲存介質的例子包括，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)、電子抹除式可複寫唯讀記憶體(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，磁帶磁片儲存或其他磁性存放裝置

或任何其他非傳輸介質，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，電腦可讀介質不包括非暫存電腦可讀媒體 (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。

本領域中具有通常知識者應明白，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介質（包括但不限於磁碟記憶體、CD-ROM、光學儲存器等）上實施的電腦程式產品的形式。

以上所述僅為本發明的實施例而已，並不用於限制本發明，對於本領域中具有通常知識者來說，本發明可以有各種更改和變化。凡在本發明的精神和原則之內，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】

S101-S404：步驟

500：檢測弱密碼的裝置

501：接收模組

502：獲取模組

503：檢測模組

504：確定模組

第 103132984 號　　民國 107 年 6 月 13 日修正

公告本

I640890

發明摘要

※申請案號：103132984

※申請日：103 年 09 月 24 日　　**※IPC 分類：** *G06F 21/46* (2013.01) *G06F 21/31* (2013.01)

【發明名稱】(中文/英文)

檢測弱密碼的方法和裝置

【中文】

本發明提供一種檢測弱密碼的方法和裝置，該方法包括：接收待測密碼；獲取所述待測密碼的用戶的身份資訊集合，所述身份資訊集合中包含所述用戶及其相關用戶的多個身份資訊；檢測所述身份資訊集合中是否存在與所述待測密碼相關的身份資訊；如果所述身份資訊集合中存在與所述待測密碼相關的身份資訊，則確定所述待測密碼是弱密碼。採用本發明的技術方案，能夠檢測待測密碼是否是用戶利用自己的身份資訊或者與自己聯繫密切的用戶的身份資訊設置的，進而判斷待測密碼是否容易破解，進一步提高用戶密碼的安全性。

【英文】

申請專利範圍

1. 一種檢測弱密碼的方法，其特徵在於，包括：

接收待測密碼；

獲取身份資訊集合，其包含該待測密碼的用戶及其相關用戶的多個身份資訊，其中該相關用戶包含至少一或多個基於該用戶的互動活動與瀏覽活動的行為資料之至少一者而決定的相關用戶；

檢測該身份資訊集合中是否存在與該待測密碼相關的身份資訊；

如果該身份資訊集合中存在與該待測密碼相關的身份資訊，則確定該待測密碼是弱密碼。

2. 根據請求項 1 所述的方法，其中，獲取該待測密碼的用戶的身份資訊集合，包括：

獲取該用戶的一個或多個身份資訊及該一個或多個相關用戶中每個相關用戶的一個或多個身份資訊，以形成該用戶的身份資訊集合。

3. 根據請求項 1 所述的方法，其中，檢測該身份資訊集合中是否存在與該待測密碼相關的身份資訊，包括：

將該身份資訊集合中的每個身份資訊按照該待測密碼的長度分別拆分成一個或多個檢測密碼；

判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與該待測密碼相同的檢測密碼；

如果任意一個身份資訊拆分成的一個或多個檢測密碼中存在與該待測密碼相同的檢測密碼，則確定該身份資訊

與該待測密碼相關。

4. 根據請求項 3 所述的方法，其中，判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與該待測密碼相同的檢測密碼，包括：

利用特定金鑰分別對該一個或多個檢測密碼進行加密，產生該一個或多個檢測密碼對應的一個或多個檢測密文；

判斷該一個或多個檢測密文中是否存在與該待測密碼的密文相同的檢測密文，其中，該待測密碼的密文是利用該特定金鑰對該待測密碼進行加密產生的；

如果該一個或多個檢測密文中存在與該待測密碼的密文相同的檢測密文，則確定該一個或多個檢測密碼中存在與該待測密碼相同的檢測密碼。

5. 一種檢測弱密碼的裝置，其特徵在於，包括：

接收模組，用於接收待測密碼；

獲取模組，用於獲取身份資訊集合，其包含該待測密碼的用戶及其相關用戶的多個身份資訊，其中該相關用戶包含至少一或多個基於該用戶的互動活動與瀏覽活動的行為資料之至少一者而決定的相關用戶；

檢測模組，用於檢測該身份資訊集合中是否存在與該待測密碼相關的身份資訊；

確定模組，用於如果該身份資訊集合中存在與該待測密碼相關的身份資訊，則確定該待測密碼是弱密碼。

6. 根據請求項 5 所述的裝置，其中，該獲取模組，

包括：

身份資訊獲取模組，用於獲取該用戶的一個或多個身份資訊及該一個或多個相關用戶中每個相關用戶的一個或多個身份資訊，以形成該用戶的身份資訊集合。

7. 根據請求項 5 所述的裝置，其中，該檢測模組，包括：

拆分模組，用於將該身份資訊集合中的每個身份資訊按照該待測密碼的長度分別拆分成一個或多個檢測密碼；

判斷模組，用於判斷每個身份資訊拆分成的一個或多個檢測密碼中是否存在與該待測密碼相同的檢測密碼；

第一確定模組，用於如果任意一個身份資訊拆分成的一個或多個檢測密碼中存在與該待測密碼相同的檢測密碼，則確定該身份資訊與該待測密碼相關。

8. 根據請求項 7 所述的裝置，其中，該判斷模組，包括：

產生子模組，用於利用特定金鑰分別對該一個或多個檢測密碼進行加密，產生該一個或多個檢測密碼對應的一個或多個檢測密文；

判斷子模組，用於判斷該一個或多個檢測密文中是否存在與該待測密碼的密文相同的檢測密文，其中，該待測密碼的密文是利用該特定金鑰對該待測密碼進行加密產生的；

確定子模組，用於如果該一個或多個檢測密文中存在與該待測密碼的密文相同的檢測密文，則確定該一個或多

個檢測密碼中存在與該待測密碼相同的檢測密碼。

【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