201837764

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201837764 A

(43)公開日： 中華民國 107 (2018) 年 10 月 16 日

(21)申請案號：107106252 (22)申請日： 中華民國 107 (2018) 年 02 月 23 日

(51)Int. Cl.： *G06F21/32 (2013.01)* *H04L9/32 (2006.01)*

(30)優先權：2017/02/24 美國 62/463,115

(71)申請人：普雷格 霍華 (美國) PRAGER, HOWARD (US)
美國

(72)發明人：普雷格 霍華 PRAGER, HOWARD (US)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：20 項 圖式數：7 共 58 頁

(54)名稱

生物特徵感測器

BIOMETRIC SENSOR

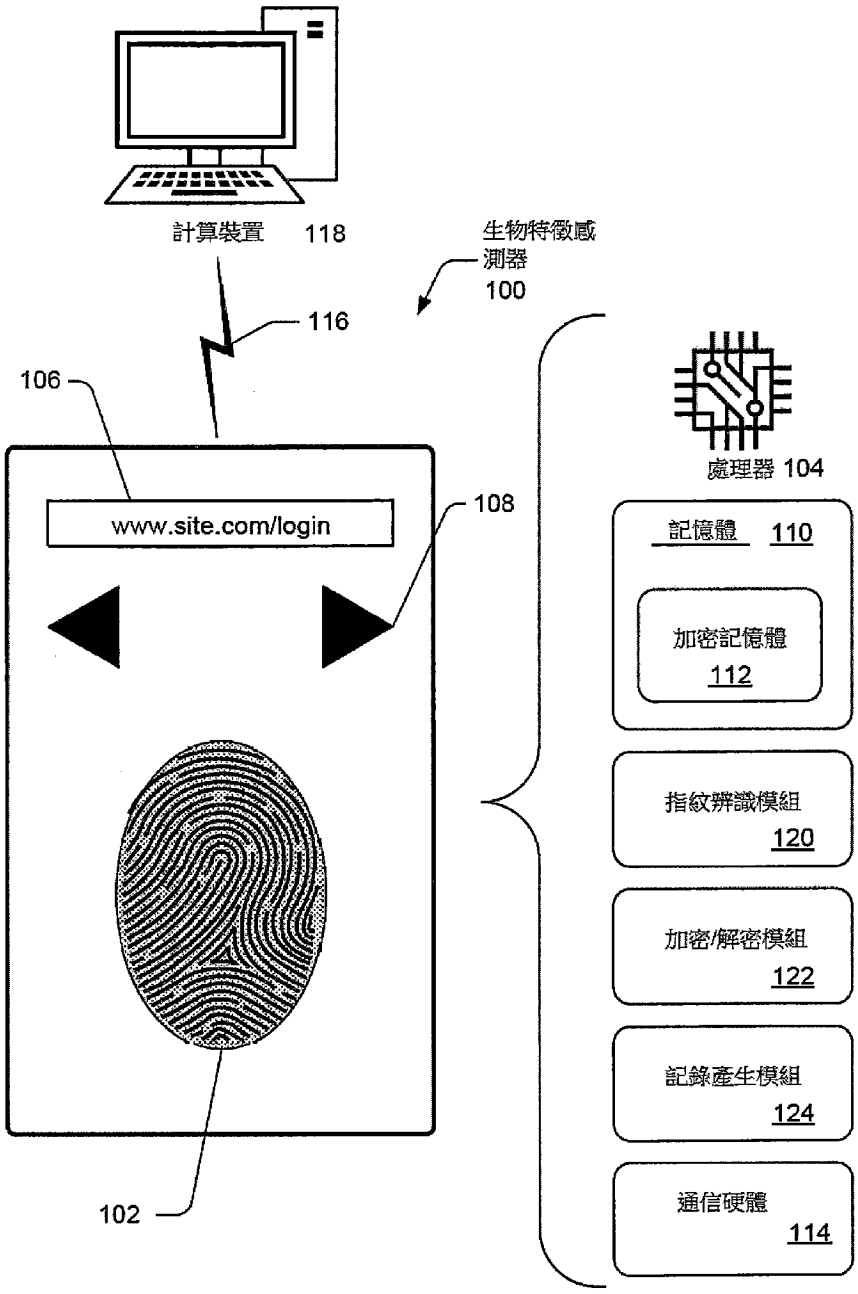
(57)摘要

一種生物特徵識別裝置可用以保護密碼及其他有價值之資訊。在一個實施方案中，該生物特徵識別裝置可為一電容式指紋感測器。電容讀數可用以識別一指紋之脊部及谷部且判定與該指紋感測器接觸之一物件是否為活組織。可藉由辨識生物特徵輸入之真實性及提供該等生物特徵輸入之一特定組合或序列而實施雙因素識別。提供一使用者介面，其中生物特徵輸入之序列與命令相關聯。一使用者可藉由提供一預定指紋序列至一指紋掃描儀而指示一命令。

A biometric identification device may be used to secure passwords and other valuable information. In one implementation, the biometric identification device may be a capacitive fingerprint sensor. Capacitive readings may be used to identify the ridges and valleys of a fingerprint and determine if an object contacting the fingerprint sensor is living tissue. Two- factor identification may be implemented by recognizing the authenticity of biometric inputs and a specific combination or sequence in which the biometric inputs are provided. A user interface is provided in which sequences of biometric inputs are associated with commands. A user may indicate a command by providing a predetermined sequence of fingerprints to a fingerprint scanner.

指定代表圖：

TW 201837764 A



【圖 1】

符號簡單說明：

100・・・生物特徵感測器

102・・・感測墊

104・・・處理器

106・・・顯示器

108・・・輸入裝置

110・・・記憶體

112・・・加密記憶體

114・・・通信硬體

116・・・通信連接

118・・・外部運算裝置

120・・・指紋辨識模組

122・・・加密/解密模組

124・・・記錄產生模組

【發明說明書】

【中文發明名稱】生物特徵感測器

【英文發明名稱】BIOMETRIC SENSOR

【技術領域】

本申請案係關於感測器，且更特定而言係關於生物特徵感測器。

【先前技術】

【0001】 生物特徵感測器用以確認使用者之身分。存在許多類型之生物特徵感測器，諸如指紋掃描儀、掌紋掃描儀、虹膜掃描儀等。關於生物特徵感測器之已知問題包括不能區別具有相同的生物特性之同卵雙胞胎以及易於諸如藉由使用指紋之副本以欺騙指紋掃描儀來進行「電子欺騙」。

【0002】 以比標準密碼更穩健之方式可靠地確認使用者身分在並非由中央當局管理之交易及協議(諸如例如編碼在區塊鏈中之加密貨幣及智慧合約)中將變得日益重要。在此等類型之互動中使用基於生物特徵之身分以驗證使用者將增大區塊鏈或其他同級系統中之可課責性及信賴度。

【0003】 對包括敏感的個人或金融資料之網路的駭侵亦已變成普遍問題。用於將對網路之存取限於僅受識別之使用者的系統可用以藉由防止未知或未經認證之使用者存取而排除駭客並增加網路、網站等之安全性。

【發明內容】

【0004】 提供本發明內容以按照簡化形式引入一些概念，該等概念在下文實施方式中進行進一步描述。本發明內容既不意欲識別所主張之標的之關鍵特徵或基本特徵，亦不意欲用以限制所主張之標的之範疇。

【0005】 說明性生物特徵感測器可整合至具有例如類似於安全符記、隨身碟、伺服器鑰、鑰煉等之形式因子的攜帶型裝置中。生物特徵感測器可實施為使用光學、電容或其他技術以感測指紋上之脊部及谷部之景貌的指紋感測器。

生物特徵感測器可包括儲存諸如文數字密碼串、信號卡號碼、銀行帳號等之值的加密記憶體。在說明性使用情形中，生物特徵感測器可通信地連接至運算裝置且自運算裝置接收字串，諸如例如運算裝置上當前顯示之網站的統一資源定位器(URL)。回應於接收諸如指紋之經認證之生物特徵輸入，生物特徵感測器可解密與URL相關聯之加密密碼且提供該密碼至運算裝置上之網頁瀏覽器。用以實施此技術之裝置可稱作例如「智慧密碼隨身碟」。

【0006】 可類似於或不同於智慧密碼隨身碟之生物特徵感測器可用以藉由辨識多個生物特徵輸入及彼等輸入之特定序列來提供雙因素識別。例如，若生物特徵輸入為指紋，則用於提供雙因素生物特徵識別之技術可包括接收第一指紋及第二指紋，接著比較每一指紋與所儲存資料以判定所感測之指紋與同經認證之指紋相關聯之所儲存資料是否相匹配。提供兩個指紋之順序至生物特徵感測器作為用以產生命令或解鎖功能性之第二因素。作為實例，若使用者將用其右手食指隨後用其左手拇指觸碰生物特徵感測器，則雙因素識別將判定右手食指及左手拇指之指紋與使用者之所保存的指紋資料相匹配且給定命令之預定義時間順序指定首先為右手食指且其次為左手拇指。因此，具有指紋之副本的同卵雙胞胎或罪惡的使用者仍將需要知道呈現指紋之順序以便產生命令或解鎖功能性。

【0007】 本文中揭示之裝置及系統的特徵可在生物特徵感測器自身及/或在諸如伺服器或其他實體遠端系統之另一運算裝置中實施。此等系統可提供具有至諸如銀行、信用卡、加密貨幣帳戶等多個不同服務提供者之連結的使用者介面(UI)，其中個別連結與指紋型樣之特定組合相關聯。因此，例如，左手無名指繼之以左手食指可存取至使用者之銀行帳戶的連結。由生物特徵感測器偵測之指紋的時間順序可為識別組合之一部分。因此，繼續先前之實例，按不同順序使用相同手指(即，左手食指繼之以左手無名指)並不存取使用者之銀行帳戶但

可存取不同帳戶。

【0008】 可在生物特徵感測器與單獨的運算裝置之間進行傳輸期間對用以存取此連結之指紋型樣加密。接收加密指紋型樣之運算裝置可使用指紋加密/解密模組以未加密所傳輸信號並產生未加密之指紋型樣。接收指紋型樣之運算裝置可存取主指紋記錄或其他資料儲存器中之所保存的指紋型樣且可使用生物特徵認證模組以比較未加密之指紋型樣與所儲存型樣以便判定是否匹配。可基於指紋與經認證指紋相匹配的判定及生物特徵感測器偵測指紋型樣之順序產生存取連結中之一者的命令。

【圖式簡單說明】

【0009】 參考附圖描述了詳細描述。在圖式中，參考符號之最左位數識別該參考符號首次出現之圖式。不同圖式中之相同參考符號指示類似或相同的項。

【0010】 圖1為說明性生物特徵感測器之示意圖。

【0011】 圖2示出了包括指派給使用者之手指的指紋之數值的說明性UI。

【0012】 圖3為包括生物特徵感測器之說明性網路環境的示意圖。

【0013】 圖4為處理自生物特徵裝置接收之資料之伺服器電腦的說明性方塊圖。

【0014】 圖5為示出多個圖示之說明性UI，該等圖示表示可由生物特徵輸入之特定組合或序列存取的連結。

【0015】 圖6為基於指紋認證提供密碼至網站之說明性過程的流程圖。

【0016】 圖7A及7B為基於雙因素指紋偵測產生命令之說明性過程的流程圖。

【實施方式】

相關申請案之交叉參考

【0017】 本申請案主張2017年2月24日提交之標題為「Intelligent Thumbdrive

and Holster Solution」之美國臨時專利申請案序列號62/463115的權益，該臨時專利申請案明確地以引用之方式整體併入本文中。

【0018】 圖1為生物特徵感測器100之示意圖。生物特徵感測器可實施為任何類型之生物特徵感測器，諸如指紋掃描儀、視網膜掃描儀、掌紋掃描儀等。在實施方案中，生物特徵感測器100包括用於偵測指紋之感測墊102。存在可用以感測指紋之多種不同技術，包括光學、電容及超聲。

【0019】 指紋感測可偵測人類皮膚上之脊部及谷部的型樣，該等脊部及谷部對應於指紋之與感測墊102接觸的一部分。由感測墊102產生之信號可包括點的景貌，該等點各自與感測墊102上之位置(例如，x及y值)任何所偵測值(諸如光或電容)相關聯。此產生表示指紋之點的景貌。具有足夠解析度之感測器亦將讀取在指紋谷部中之每一者的側面內及上之點處的電容。所偵測點之總數目的特定子集可用以按以下方式表示景貌，該方式捕獲景貌之最獨特的態樣及/或減少儲存指紋之表示所需的資料量。例如，穿過景貌點之預定路徑可用以識別隨後經採用作為指紋之代表的點之子集。

【0020】 電容式指紋感測器可由含有微型單元之陣列的一或多個半導體晶片構成。每一單元包括以絕緣層覆蓋之兩個導體板。單元小於指紋上之一個脊的寬度。電容式指紋感測器可連接至積分器，一種建構在反相運算放大器周圍之電路。反相放大器為由若干電晶體、電阻器及電容器構成之複雜的半導體裝置。反相放大器更改供應電壓。該更改係基於稱作反相端子及非反相端子之兩個輸入的相對電壓。在此情況下，非反相端子連接至接地，且反相端子連接至參考電壓供應器及反饋迴路。反饋迴路包括兩個導體板，反饋迴路亦連接至放大器輸出。手指之表面充當第三電容器極板，第三電容器極板藉由單元結構中之絕緣層且在指紋谷部之情況下為氣穴分隔。改變電容器極板之間的距離(藉由將手指移動靠近或遠離導體板)會改變電容器之總電容(儲存電荷之能力)。由於

此品質，在脊部下方之單元中的電容器與在谷部下方之單元中的電容器相比將具有較大電容。

【0021】 為了掃描手指，生物特徵感測器100之處理器104首先閉合每一單元之重置開關，此使每一放大器之輸入及輸出短路以「平衡」積分器電路。當開關再次斷開且處理器104將固定電荷施加至積分器電路時，電容器充電。反饋迴路之電容器的電容影響放大器之輸入處的電壓，放大器之輸入處的電壓影響放大器之輸出。由於與手指之距離會更改電容，因此手指脊部將導致與手指谷部不同之電壓輸出。處理器104讀取此電壓輸出且判定其為脊部抑或谷部之特性。藉由讀取感測器陣列中之許多單元，處理器104可拼湊出指紋之整體圖像——景貌。

【0022】 電容式指紋感測器之一個實例為可自中國廣東之JP Sensor Corp. Ltd.購得的JP2380感測器模組。電容式指紋感測器之另一實例為可自中國深圳之INJES Technology Co., Ltd.購得的INJES FRT1012拇指印讀取器。

【0023】 在實施方案中，生物特徵感測器100可包括兩個或更多個感測墊102。多個感測墊102可藉由允許同時偵測及確認兩個不同的指紋而增加安全性且可允許較方便的使用者介面，其中使用者可使用一個感測墊102以用於左手之手指且使用另一感測墊102以用於右手之手指。在一個實例中，生物特徵感測器100可包括10個單獨的感測墊102，使得針對使用者之10個手指中之每一者存在一個感測墊102。

【0024】 電容式感測可用以區分由活組織產生之指紋與由非活組織產生之指紋或指紋之三維副本。例如，Keizou Takamatsu，*Resistance and Capacitance of the Human Scan at the Transient and Instant Condition Applied by the Finite Alternating Potential*，Shigaku 76(7): 1412-1423，1989中描述了用於識別人類皮膚之電阻及電容的一種技術。將有限交流電施加至活體可自經過電位之振幅及

相位角的變化產生電阻及電容值。藉由此方法，可針對將每一頻率施加至活體之暫態及常態量測電阻及電容。經組態以使用例如Takamatsu描述之技術將有限交流電施加至指尖的感測墊102可偵測與感測墊102接觸之物件的回應是否表現得與活組織一致。此外，溫度及/或濕度對指紋景貌之脊部、谷部及谷部側面之間的電容值差異之影響可用以識別展現活組織之特性的電容讀數。例如，指紋之脊部上溫度較低且谷部中之溫度相對較高為活組織之特性，該特性在指紋之合成複製品中可能不存在。因此，基於指紋之脊部與谷部之間的濕度及/或溫度之差異的活組織之已知特性可用以判定感測墊102上之指紋讀數是否為活組織產生的。

【0025】 另外，用於辨別活組織與非活組織之以上技術中之任一者可使用諸如分類器之機器學習技術及訓練資料集合進行訓練，訓練資料集合由來自活人之實際指紋及由石蠟、乳膠或其他材料製成的指紋之合成副本組成。因此，藉由提供適當的訓練資料至機器學習分類器，電腦系統可學習如何將電容讀數分類為與活組織相關聯之讀數及與活組織無關聯之讀數。用於訓練電腦系統以將新輸入分類至多個類別中之一者的機器學習技術對於一般熟習此項技術者而言為眾所周知的。下文附錄A中包括了關於Takamatsu中描述之技術的額外細節。一般熟習此項技術者將理解如何調適本文中描述之硬體及軟體以實施附錄A中之技術。

【0026】 生物特徵感測器100可實施為可隨使用者方便地移動之手持型或攜帶型裝置。在一個實施方案中，生物特徵感測器100可包括能夠顯示諸如ASCII字元之文字的顯示器106。顯示器可實施為液晶顯示器、電子紙顯示器、發光二極體(LED)顯示器，或其他顯示技術。生物特徵感測器100亦可包括輸入裝置108，諸如一或多個按鈕、開關、滾輪等，其在用於輸入裝置108時可改變顯示器106上顯示之資訊，顯示器106上顯示之資訊又可改變自生物特徵感測器100

傳輸至其他裝置之資料。生物特徵感測器100可包括電源，諸如電池。

【0027】 生物特徵感測器100本身可為包括處理器104及記憶體110之運算裝置。記憶體110可包括加密記憶體112。加密記憶體112可用以儲存敏感資料，諸如密碼、信用卡號碼、銀行帳號、用於存取加密貨幣帳戶之散列，及其類似者。儲存在加密記憶體112中之每一加密值可與字串(諸如，使用密碼之網站的URL或發出信用卡之銀行的名稱)相關聯。因此，加密值之「名稱」可顯示在顯示器106中。顯示器106不顯示密碼或信用卡號碼本身，而是顯示諸如將允許使用者識別哪一密碼、信用卡號碼等當前可用於自生物特徵感測器100進行存取之「名稱」的資訊。

【0028】 生物特徵感測器100亦可包括用於與外部運算裝置118建立通信連接116之通信硬體114。通信硬體114可為經組態以產生諸如用於任何已知無線通信技術之信號之無線電或電子信號的數據機，無線通信技術包括藍芽、Wi-Fi(例如IEEE 802.11)、蜂巢式資料，或近場通信(例如，Ecma- 340、ISO/IEC 18092)。通信硬體114可另外地或可選地提供用於使用用於運算裝置之任何已知類型之纜線或連接技術(諸如通用串列匯流排(USB)纜線、火線纜線、耳機纜線、電話纜線等)來實施有線連接的埠、插頭、插座等。因此，通信連接116可為有線或無線連接。運算裝置118可實施為任何類型之運算裝置，諸如桌上型電腦、膝上型電腦、平板電腦、智慧型電話、個人數位助理等。

【0029】 指紋辨識模組120可包括在生物特徵感測器100中。指紋辨識模組120可比較由感測墊102產生之信號與生物特徵感測器100上儲存之資料。例如，可將由知道係經認證之使用者之指紋掃描產生的資料儲存在加密記憶體112中。所儲存之資料可為表示所掃描指紋之景貌的一系列值或其某一子集，諸如對應於穿過構成景貌之多個點之預定路徑的值。指紋辨識模組120可使用任何已知的或尚待開發之技術以用於判定由感測墊102所感測之指紋與經認證

之指紋是否相匹配。活組織與非活組織之間的辨別亦可由指紋辨識模組120使用例如諸如由Takamatsu描述之演算法、由機器學習開發之演算法，或不同技術實行。因此，指紋辨識模組120可判定給定指紋為經認證之指紋且由活組織產生。

【0030】 加密/解密模組122可控制對加密記憶體112或儲存在記憶體110中之加密資料的存取。用於對資料加密之任何合適的技術可用以保護加密記憶體112。在一些實施方案中，加密可由諸如安全密碼處理器之專用硬體提供。安全密碼處理器可實施為嵌入於具有多個實體安全措施之包裝中的用於執行保密操作之晶片或微處理器上的專用電腦，該等安全措施提供某一抗竄改程度至該電腦。在判定與感測墊102接觸之指紋為經認證之指紋後，加密/解密模組122可解密儲存在加密記憶體112中之資料的全部或一部分。

【0031】 對加密值的解密產生並非加密之值。如上文所描述，此值可為密碼、信用卡號碼、散列碼，或其類似者。可基於顯示器106中顯示之資訊來識別經加密之值。因此，若顯示器106中顯示「www.site.com/login」，則值可對應於用以登錄該網站之密碼。

【0032】 諸如網址之字串與特定加密值之間的對應可儲存在記憶體110及/或加密記憶體112中。例如，加密記憶體112可儲存字串及相關聯之值(諸如密碼或信用卡號碼)之查找表。在一個實施方案中，諸如信用卡之「名稱」或網站之URL之非安全資訊可儲存在記憶體110中，存儲器110具有至加密記憶體112中之特定位置的指示器。且加密記憶體112中之對應位置儲存加密值，諸如密碼或信用卡號碼。

【0033】 因此，在接收字串後，加密/解密模組122可解密與該字串對應之值。加密記憶體112之其他內容可保持為加密的。在一個實施方案中，用以識別待未加密之值的字串可顯示在顯示器106中。使用者可藉由操縱輸入裝置108

來改變顯示器106上顯示之字串，且因此改變未加密之值。

【0034】 在不同實施方案中，字串可由運算裝置118提供。例如，生物特徵感測器100可基於運算裝置118上打開之網頁瀏覽器中顯示之URL而經由通信連接116自運算裝置118接收字串。因此，運算裝置118可將對用以訪問當前在網頁瀏覽器中顯示之網站之密碼的請求傳達至生物特徵感測器100。

【0035】 記錄產生模組124可在記憶體110及/或加密記憶體112中創建字串與值之間的關聯之記錄。記錄產生模組124將新資料添加至生物特徵感測器100，使得可儲存新網站之密碼或新信用卡之號碼。例如，若生物特徵感測器100與運算裝置118進行通信連接且訪問了在生物特徵感測器100之記憶體110中無對應項的網站，則網站之URL及由使用者手動鍵入之密碼可由生物特徵感測器100記錄。記錄產生模組124接著可創建至少部分經加密之記錄，該記錄將網站之URL與密碼關聯地進行儲存的。類似地，使用者可在運算裝置118上鍵入新信用卡之信用卡號碼及信用卡之名稱且可藉由生物特徵感測器100上之記錄產生模組124創建將信用卡號碼與名稱相關聯之記錄。在隨後訪問網站時，使用者可提供他或她的指紋至生物特徵感測器100，以便解密並向運算裝置118提供適當的密碼以用於登錄網站。

【0036】 圖2示出了說明性UI之圖式200，在該UI中存在第一生物特徵感測器202及第二生物特徵感測器204。第一生物特徵感測器202可主要用於讀取使用者之左手206的指紋。第二生物特徵感測器204可主要用於讀取使用者之右手208的指紋。然而，如上文所描述，類似的UI可實施為具有更大或更小數目之生物特徵感測器202/204。在此UI中，使用者之手指中之每一者，更精確而言對應指紋可與自0至9之整數相關聯。特定指紋與整數之關聯為任意的且可為使用者可組態的。在此圖式200所示之實例中，左手206之拇指與0相關聯且左手之剩餘手指與偶數整數2、4、6及8相關聯。右手208之手指與奇數整數1、3、5、

7及9相關聯。因此，特定手指組合可由數字表示。例如，數字103對於此實例表示右手拇指、左手拇指、右手食指。經選定將整數與不同手指相關聯之不同使用者將使用不同的手指組合來表示數字103。

【0037】 藉由獨特整數來表示手指之此技術允許UI之態樣(諸如螢幕上顯示之圖示)以數字序列而非手指之清單呈現。例如，若使用者將用於解鎖電子資料夾之碼設定為三個不同指紋之特定序列，則該碼可在UI上表示為三位數字而非指定使用哪些手指之冗長且較不緊密的表示。用於表示特定指紋項之此簡寫技術在存在有限螢幕空間之UI(諸如行動裝置)上可特別有用。

【0038】 另外，因為整數與手指之對應可為使用者可組態的，所以知道對應可提供第二因素以用於更安全的鑑別。例如，若UI指示鍵入103將對電子檔案解鎖，則使用者將必須知道哪些手指對應於整數1、0及3，以便提供正確的一系列指紋。然而，若UI指示使用者「掃描你的右手拇指，接著你的左手拇指，且接著你的右手食指」，則將不存在第二因素，且例如具有相同指紋之未經認證之使用者可存取電子檔案。

【0039】 雙因素鑑別可由指紋之組合及順序兩者提供。在具有多個生物特徵感測器202/204之實施方案中，同時呈現之指紋的組合可用作第二因素。例如，特定解鎖命令可由將左手中指與生物特徵感測器202接觸且將右手中指與生物特徵感測器204接觸組成。基於多個指紋之同時呈現的命令可稱作「和絃」。和絃可用作使用兩個或更多個生物特徵感測器202/204之任何實施方案上的第二因素。

【0040】 使用者可指定他或她的手指中的一或多個作為「緊急情況」或「911」手指，該手指在由生物特徵感測器202/204中之一者偵測到時產生聯繫權責機關之警示及/或防止存取由生物特徵感測器202/204保護之任何資源。例如，使用者可指定左手無名指作為「緊急情況」手指。若偵測到來自該手指之

指紋，則使用指紋識別之系統可進入警示狀態。使用「緊急情況」手指提供使使用者諸如例如在被迫使用他或她的生物特徵來准予存取時秘密地指示他或她處於脅迫下的技術。藉由其中需要多個不同手指以用於互動之UI，不知道哪個手指觸發警示狀態之壞人將不知道使用者是否使用了「緊急情況」手指以產生警報。類似地，即使壞人操縱無意識之使用者之手指或使用能夠欺騙生物特徵感測器202/204的指紋之副本，壞人10次中將有一次機會使用「緊急情況」手指並且無意中警示權責機關。

【0041】 圖3示出了包括生物特徵感測器302之說明性網路環境300。生物特徵感測器302可與圖1中介紹之生物特徵感測器100相同或類似。生物特徵感測器302可藉由通信連接306連接至多個不同類型之運算裝置304(A)、304(B)或304(C)(統稱為304)中之任一者，通信連接306可使用有線或無線技術實施。生物特徵感測器302可具有攜帶型形式因子，使得其可由使用者攜帶並在不同時間連接至不同運算裝置304。例如，使用者可在在家中時將生物特徵感測器302連接至第一運算裝置304(A)以提供生物特徵鑑別且在不在家中時將生物特徵感測器302連接至第二運算裝置304(C)。

【0042】 運算裝置304可連接至網路308。網路308表示任何類型之通信網路，諸如網際網路、廣域網路(WAN)、區域網路(LAN)、電話網路、纜線網路、網狀網路、同級網路及其類似者。網路308提供與諸如伺服器310或網站伺服器314之一或多個其他實體遠端運算裝置的連接。伺服器310可實施為單一不同的實體裝置或可表示一起共同提供網路運算功能性之多個不同裝置的一部分。因此，伺服器310可實施為跨域一或多個不同的實體位置分佈之複數個伺服器或其他運算裝置。伺服器310亦可表示用於使得能夠對可組態資源(諸如電腦網路、伺服器、儲存器、應用程式及服務)之共用池進行普遍存在之存取的「雲端」運算基礎架構及軟體模型，該等可組態資源可經由網路308提供。網

站伺服器314可提供網頁及其他資料至運算裝置304。例如，網站伺服器314可回應於由網頁瀏覽器或其他HTTP客戶端轉發之請求而使用諸如超文件傳送協定(HTTP)之標記語言來提供形成網頁之檔案至運算裝置304。

【0043】 伺服器310可包括實行後端處理以驗證或鑑別由生物特徵感測器302接收之生物特徵資料的生物特徵認證模組312。因此，在一些實施方案中，伺服器310上之硬體及軟體判定所偵測之指紋與經認證之指紋是否相匹配。伺服器310亦可與諸如網站伺服器314之其他運算裝置通信且基於自生物特徵感測器302接收之生物特徵資料的確認而提供認證。例如，若生物特徵認證模組312判定由生物特徵感測器302偵測之生物特徵資料與經認證之使用者的生物特徵資料相匹配，則伺服器310可提供充當經認證之使用之證據的符記至網站伺服器314。將生物特徵認證功能性置於伺服器310上而非生物特徵感測器302上降低對生物特徵感測器302之運算需求，此可允許較小之形式因子或較便攜之裝置。另外，若對生物特徵認證技術之態樣的更新可應用於單一伺服器310而非許多不同的生物特徵感測器302，則該更新可簡化。

【0044】 圖4示出了伺服器310內之組件的說明性方塊圖400。儘管在圖式400中一起以單一群示出，但應理解，伺服器310之各種組件可跨越多件硬體及多個實體位置分佈。伺服器310可包括一或多個處理器402及記憶體404，記憶體404儲存各種模組、應用程式、程式或其他資料。處理器402中之個別處理器可實施為硬體處理單元(例如，微處理器晶片)或軟體處理單元(例如，虛擬機)。硬體處理單元可實施為具有任何合適類型之處理器，諸如單核處理器、多核處理器、中央處理單元(CPU)、圖形處理單元(GPU)，或其類似者。記憶體404可包括當由一或多個處理器402執行時使處理器402實行本文中所描述之操作的指令。伺服器310亦可包括用於儲存諸如密碼、信號卡號碼及其類似者之資料的加密記憶體406。伺服器310亦可包括與網路308或其他網路之網路連接408，諸

如網路介面卡或數據機。

【0045】 記憶體404可包括在硬體或韌體中實施之電腦可讀媒體。記憶體可包括但不限於RAM、ROM、EEPROM、快閃記憶體或其他記憶體技術、CD-ROM、數位多功能光碟(DVD)或其他光學儲存器、磁卡、磁帶、磁碟儲存器或其他磁性儲存裝置，或可用以儲存資訊且可由處理器存取之任何其他有形媒體。電腦可讀媒體涵蓋非暫時性電腦可讀媒體。非暫時性電腦可讀媒體包括除了暫時性信號之外的所有類型之電腦可讀媒體。

【0046】 伺服器310亦含有多個模組。該等模組可實施為儲存在記憶體404(或其他地方)中之軟體、韌體、硬體、系統單晶片(SOC)、機械運算裝置等。

【0047】 指紋加密/解密模組410可解密表示加密指紋型樣之資料。指紋型樣，脊部及谷部之景貌可以加密形式傳輸至伺服器310，使得對傳輸之攔截將不會提供可用以阻止生物特徵安全措施之資料。多個不同類型之加密技術可用以在傳輸期間對指紋加密，諸如公共/私人秘鑰加密或在生物特徵感測器及伺服器310兩者上使用密碼處理器。亦可藉由散列化表示指紋型樣之資料或經由以任意資料或雜訊進行相加或相減而組合指紋型樣來實施加密。

【0048】 在一個實施方案中，可使用合成生物特徵資料對發送至伺服器310之指紋或其他生物特徵資料加密。合成生物特徵資料可在生物特徵感測器處與所感測資料組合。用於實施組合之技術可包括加法、減法、乘法或用於組合兩個資料集合之其他已知技術。因此，離開生物特徵感測器之信號並非自指紋掃描儀或其他類型之感測器收集的原始資料，而是已藉由合成生物特徵資料混淆之資料。在不知道如何操縱所感測資料之情況下，可能不可能自傳輸重新產生原始資料。

【0049】 用以模糊生物特徵讀數之合成的生物特徵資料可具有與實際生物特

徵資料類似之特性。但是合成資料不對應於實際生物特徵讀數。在電容式指紋掃描之情況下，合成生物特徵資料可為任意電容值之景貌。景貌可部分藉由使用隨機數以創建電容值之集合而產生。然而，合成生物特徵資料中包括之值可受約束，使得其類似於實際生物特徵量測中識別之值。例如，對指紋之電容式掃描可產生落在特定值範圍內之電容值且掃描表面之不同部分可具有不同的值範圍。例如，朝向指紋進行較有力之接觸之感測器中間的電容值可較高，且在手指不接觸感測器表面之邊緣處值較低或為零值。合成地產生之任意指紋型樣可經設計以具有類似特徵。如此做之一種方式為組合來自大量單獨生物特徵量測之值。此將創建具有中位差及標準差之值的分佈。由實際量測得到之此等統計值可用以諸如藉由將合成值限於實際值之特定子集來約束合成值。例如，對於景貌上之給定x、y位置，隨機選擇之電容值可受限於僅在同一x、y位置處之實際指紋電容之中位值的一個標準差、兩個標準差，或三個標準差內之值。因此，合成生物特徵資料可包括隨機值，但將具有對於實際生物特徵資料為典型之值。

【0050】　可產生大量合成生物特徵資料集合。例如，可產生電容值之1000、10000、100000或更多個不同的人造景貌。合成生物特徵資料之副本可儲存在生物特徵感測器及伺服器310兩者上。資料自生物特徵感測器至伺服器310之每一傳輸可使用不同的人造景貌來加密。人造景貌用以對傳輸加密之順序可為預定的。例如，自生物特徵感測器發送至伺服器310之第一指紋掃描可使用合成地產生之任意指紋型樣#1207進行編碼。因此，在接收該第一傳輸後，指紋加密/解密模組410將使用型樣#1207以對加密指紋解碼。

【0051】　伺服器310上存在之合成生物特徵資料的集合可用於多個使用者。然而，對於每一使用者，使用合成型樣之順序可不同。因此，與第一使用者相關聯之用以未加密來自生物特徵感測器之第n次傳輸的合成生物特徵資料將不

同於與第二使用者相關聯之用以未加密來自生物特徵感測器之第n次傳輸的生物特徵資料。因此，合成生物特徵資料及使用者之身分兩者皆用以未加密發送至伺服器310之指紋或其他生物特徵資料。

【0052】 生物特徵認證模組312比較由指紋加密/解密模組410解密之指紋型樣與所儲存之指紋型樣。若存在匹配，則生物特徵認證模組312將由生物特徵掃描儀掃描之指紋辨識為屬於經認證之使用者。生物特徵認證模組312可使用任何已知的技術以用於比較指紋掃描。生物特徵認證模組312亦可判定所感測之指紋是否由活組織產生。生物特徵認證模組312可使用先前論述之技術中之任一者，諸如藉由比較脊部及谷部電容讀數之景貌與活組織之已知特性來進行此操作。

【0053】 登記在系統中之使用者的參考指紋可儲存在主指紋記錄412中。主指紋記錄412可為多個使用者之指紋掃描的加密資料庫。來自使用者之所有10個手指的指紋掃描可儲存在主指紋記錄412中。來自使用者之指紋可在登記過程期間捕獲，在登記過程中使用者提供指紋掃描至伺服器310。登記過程亦可包括使用者提供識別身分碼至用以將指紋掃描與使用者之身分之另一態樣相聯繫的第三方。例如，使用者可遞交諸如駕駛執照、出生證明、護照等文件至例如公證人或在政府機關處並捕獲他或她的指紋。因此，使用者之姓名及其他資訊(諸如地址、駕駛執照號碼、銀行帳號、電話號碼、社會保險號碼等)可與他或她的指紋的掃描相關聯並發送至伺服器310。

【0054】 登記亦可藉由使用者提供識別身分碼至第三方且接著接收臨時碼或憑證而實施。使用者可將臨時碼或憑證鍵入至他或她的運算裝置中且接著藉由所附接之生物特徵感測器捕獲他或她的生物特徵資料。碼或憑證將會將所捕獲之生物特徵資料與使用者之識別身分碼中提供的資訊相關聯。因此，使用者之生物特徵資料的後續呈現將允許伺服器310將該使用者之行動與他或她的識別

身分碼相關聯。

【0055】 使用者可創建多個身分，每一身分與不同的識別身分碼相關聯。例如，一個身分可為與他或她的實際姓名及家庭地址相關聯之使用者的個人身分。另一身分可為亦與使用者之雇主以及公司信用卡帳戶相關聯之職業身分。匿名身分亦為可能的，其中使用者之生物特徵資料與諸如已編號銀行帳號、用於加密貨幣帳戶之散列碼或另一類型之電子帳戶之非識別身分碼相關聯。使用者可藉由呈現生物特徵資料之不同組合來登錄不同帳戶中之每一者。例如，若生物特徵資料為指紋，則指紋之第一序列可使使用者在與使用者之一或多個公眾已知之特性相關聯的公開身分下登錄伺服器310，且指紋之第二不同序列可使使用者在與使用者之公眾已知之特性無關聯的匿名身分下登錄伺服器310。

【0056】 伺服器310中之使用者介面(UI)模組414可產生使伺服器310或不同的運算裝置(諸如例如運算裝置118或304)產生UI之資料。UI可為使用者藉由提供生物特徵資料而與之交互的UI。例如，替代於按壓鍵盤上之鍵、觸碰觸控螢幕，或點擊鼠標，UI可呈現藉由提供特定生物特徵資料而選擇或啟動之多個圖示。例如，指紋之特定組合可用以啟動UI中之連結，UI用以指示使用者希望啟動哪個連結且提供用於存取該連結之生物特徵認證。圖5中示出了可由UI模組414產生之UI的一個實例。

【0057】 伺服器310上之所儲存資料提供模組416可在接收生物特徵認證後提供所儲存資料至其他運算裝置。例如，所儲存資料可為密碼、信用卡號碼、帳號，或其類似者。所儲存資料提供模組416可在自生物特徵認證模組312接收認證後提供密碼或其他資料至諸如網站伺服器314之不同的運算裝置。因此，在一個實施方案中，具有所儲存資料提供模組416之伺服器310可用作統一密碼儲存器，其在接收生物特徵鑑別後提供適當的密碼至網站或其他運算裝置。因此，使用者無需記住個別密碼且所有密碼受使用者之生物特徵保護。其他運算

裝置，諸如可能天生不能實施生物特徵登錄之網站伺服器314可使用伺服器310來提供該特徵。伺服器310可暴露適當的應用程式設計介面(API)以允許其他裝置存取伺服器310上可獲得之生物特徵登錄功能性。亦可提供軟體開發套件(SDK)，使得其他運算裝置可使用生物特徵資料實施登錄。例如，在網站上使用者可選擇登錄框且接著經由生物特徵感測器提供生物特徵資料。可由伺服器310處置生物特徵資料之鑑別及提供認證至登錄過程。

【0058】 伺服器310可提供認證至其他運算裝置以登錄網站或存取安全資料之一種方式為藉由提供符記。符記可由符記化模組418創建及散佈。符記化在應用於資料安全時係以稱作符記之非敏感等效物取代敏感資料元素的過程，符記無外在或可利用的意義或值。符記為經由符記化系統映射回敏感資料之參考(即，識別符)。自原始資料至符記之映射使用以下方法，該等方法使得符記在無例如使用自隨機數創建之符記之符記化系統的情況下逆轉為不可行的。當符記代替系統中之活資料時，結果為敏感資料對該等應用程式、儲存器、人及過程之暴露減到最小，從而降低了洩露或意外暴露及未經認證地存取敏感資料之風險。應用程式可使用符記以替代於活資料進行操作，例外情況為在確實必要時明確准許少量可信賴之應用程式去符記化。符記化系統可在資料中心之安全的隔離段內內部地操作或作為來自安全服務提供者之服務而操作。

【0059】 符記化模組418可創建生物特徵符記，該符記基於由生物特徵認證模組312評估之生物特徵資料而提供使用者之身分的證明。符記之接收可基於由伺服器310應用之生物特徵識別技術來辨識使用者之身分的真實性。符記化模組418可對由單獨的運算裝置或服務提供者提交之每一登錄請求發出符記回應。因此，由符記化伺服器310發出之符記可用作握手程序之一部分，握手程序將使用者之運算裝置連接至單獨的運算裝置，諸如網站伺服器314。除了握手及初始連接之外，可藉由符記化模組418提供符記以實施由生物特徵保護之

任何命令。例如，登錄銀行網站可需要第一符記且起始資金轉移可需要第二符記，第一符記及第二符記皆自伺服器310發出至銀行之運算系統。

【0060】 分配符記之角色可藉由提供主租約而自伺服器310委託給其他實體或運算裝置。主租約提供自伺服器310獲得符記以用於重新分配給其他方之權利。租約提供符記至終端使用者以供該使用者用於訪問網站或受生物特徵身分保護之其他資源。因此，由伺服器310發出之符記代表自生物特徵感測器捕獲之實際資料檔案且允許跨越較寬範圍之系統及運算裝置校驗及傳達生物特徵身分。在一些實施方案中，控制伺服器310之實體可對提供符記收取費用。例如，1/10,000分可購得單一符記。

【0061】 伺服器310亦可包括警示模組420。警示模組可基於「警示」手指之偵測而實施警示。因此，若生物特徵感測器讀取到使用者之「警示」手指的指紋，一旦提供該指紋型樣至伺服器310，則該指紋型樣可由警示模組420辨識且警示模組420可觸發警示條件。觸發警示條件可包括判定生物特徵感測器之位置及提供位置以及已觸發警示之訊息至警察或其他權責機關。警示條件亦可改變UI模組414之行為，使得UI顯示看上去為使用者與運算系統之間的標準互動之樣子但實際上不實施任何交易或存取任何安全資料。因此，UI之觀看者，可能包括試圖強迫使用者存取受生物特徵保護之資料的壞人將看到看起來為正常UI互動的樣子但實際上將不實施UI上顯示之底層改變。

【0062】 若觸發了警示條件，則該條件可持續直至警示模組420經重置且警示條件清除為止。警示模組420可藉由使用者鍵入生物特徵資料之特定序列(諸如指紋之特定序列)而重置。在一個實施方案中，警示模組可藉由使用者呈現身分碼給第三方來重置，使用者呈現身分碼與使用者可最初登記生物特徵識別服務之方式類似。第三方接著可代表使用者聯繫伺服器310或提供可用以重置警示模組420之臨時憑證或碼給使用者。

【0063】 伺服器310可包括除了上文論述之模組之外的額外模組且本文中論述之模組中之任一者可省略或進行組合。

使用者介面

【0064】 圖5示出了可由UI模組414產生之說明性UI 500。UI 500包括至服務提供者之複數個連結。連結502可例如提供至信用卡之連結。服務提供者可與金融機構或經由網際網路或其他電子通信通道與使用者互動的任何類型之服務提供者相關聯。例如，服務提供者可包括信用卡公司、銀行、線上商家、證券經紀商、提供串流媒體之網站、加密貨幣網站，或其他服務提供者，諸如用於訂購食物遞送之網站。UI 500可顯示任何數目之不同連結，諸如10個、20個、50個、100個或某一其他數目個連結。在一個實施方案中，UI 500可將連結中之每一者示出為文字框。

【0065】 連結中之個別連結可與數字相關聯。實例為「01」，其為與連結502相關聯之數字504。數字504可為包括一位數、兩位數、三位數或更多位數之整數。圖2所示之UI呈現了將數字指派給使用者之個別手指的一種方式。因此，例如，可藉由使用者將對應於數字0及數字1之手指以該順序觸碰指紋感測器來存取第一連結502。使用圖2所示之編號，將藉由使用者呈現其左手拇指之指紋，隨後其右手拇指之指紋來存取第一連結502。UI 500使用指紋之生物特徵資料以確認使用者之身分及呈現生物特徵資料之選擇，以便實施特定命令，諸如存取連結。在一些實施方案中，UI 500之組態可由使用者進行組態且他或她可選擇以哪個順序顯示哪些連結以及個別連結之對應數字。在其他實施方案中，UI 500之全部或一部分可基於控制伺服器310之實體與同所顯示連結相關聯之實體之間的關係進行結構化。一個類型之關係為付費置入，其中服務提供者可憑付款而在UI 500上特定位置呈現有其連結。除了付款之外，亦可藉由控制連結之實體可能憑對控制伺服器310之實體的付款來選擇數字504。

說明性過程

【0066】 下文論述之過程各自示出為邏輯流程圖中之區塊的集合，該等區塊表示可在硬體、軟體或其組合中實施之一系列操作。在軟體情況下，區塊表示儲存在一或多個電腦可讀媒體上之電腦可執行指令，該等電腦可執行指令在由一或多個處理單元執行時實行所述操作。一般而言，電腦可執行指令包括實行特定功能或實施特定抽象資料類型之常式、程式、物件、組件、資料結構及其類似者。描述操作之順序不意欲解釋為限制，且任何數目之所描述區塊可以任何順序及/或並行地組合以實施過程。

【0067】 圖6為使用生物特徵鑑別來擷取密碼之說明性過程600的流程圖。過程600可例如在圖3所示之網路環境300中實施，環境300具有圖1及圖3所示之裝置。當然，過程600(及本文中描述之其他過程)可在其他類似及/或不同的環境中實行。

【0068】 在602處，在諸如圖3所示之運算裝置304中之任一者的運算裝置上打開網站。在運算裝置上打開網站可包括啟動在運算裝置上運行之網頁瀏覽器應用程式及將網頁瀏覽器導向至顯示為現用視窗，與URL相關聯之網頁。網頁可包括用於諸如密碼、信用卡號碼、存取碼等之值之項的欄位、視窗、文字框或其類似者。

【0069】 在604處，將生物特徵感測器連接至運算裝置。生物特徵感測器可與圖1所示之生物特徵感測器100或圖3所示之生物特徵感測器302相同或類似。生物特徵感測器與運算裝置之間的連接可為通信連接，諸如圖3所示之通信連接306。連接為雙向連接。運算裝置及生物特徵感測器兩者皆可發送及接收資料。

【0070】 在606處，藉由生物特徵感測器自運算裝置接收網站之URL。URL可為在運算裝置上運行之網頁瀏覽器之現用視窗中當前顯示的網站之文字表

示。

【0071】 在608處，生物特徵感測器判定網站是否為已知的。若網站為已知的，則URL與密碼或其他值關聯地儲存在生物特徵感測器之記憶體中。若網站因為網站之URL不存在於查找表或生物特徵感測器內之其他資料結構中而為未知的，則過程600沿著「否」路徑進行至610。

【0072】 在610處，自將密碼鍵入至運算裝置中之使用者接收密碼項且運算裝置提供密碼至生物特徵感測器。

【0073】 在612處，可藉由生物特徵感測器對密碼加密且將其儲存在加密記憶體(諸如圖1所示之加密記憶體112)中。密碼之加密可由加密/解密模組122提供。密碼之加密亦可或亦可不對網站之該URL加密。

【0074】 在614處，將加密密碼與URL關聯地保存在生物特徵感測器上。因此，生物特徵感測器創建了密碼與網站之URL關聯的記錄。此記錄可例如由圖1所示之記錄產生模組124創建。

【0075】 若在608處URL網站為已知的，則過程600沿著「是」路徑進行至616。在616處，自記憶體(諸如，例如加密記憶體112)擷取加密密碼。

【0076】 在618處，生物特徵感測器判定是否偵測到經認證之指紋。經認證之指紋可為與使用者之與生物特徵感測器相關聯之所保存指紋相匹配的指紋。經認證之指紋可為使用者之10個指紋中之任一者或可僅為該等指紋之子集，諸如僅單一個別指紋。在一個實施方案中，經認證之指紋可為使用者之九個指紋中之任一者，但第十個指紋可用以觸發警示，且因此不辨識為經認證之指紋。可藉由圖1所示之指紋辨識模組120將指紋辨識為經認證之指紋。

【0077】 在620處，提供加密密碼至網站。因此，藉由將生物特徵感測器連接至運算裝置，使用者能夠使用他或她的指紋來存取儲存在生物特徵感測器上之密碼且提供該密碼至網站而無需手動地鍵入密碼。使用者無需記住密碼且若

網站對於生物特徵感測器為已知的，則生物特徵感測器在被呈現經認證之指紋時自動提供正確的密碼。

【0078】 圖7A及7B為使用雙因素生物特徵識別以產生命令之說明性過程700的流程圖。

【0079】 在702處，自指紋感測器接收代表第一指紋之第一信號。第一代表性信號可為由指紋感測器產生之電容或其他值的景貌。在一個實施方案中，第一信號為由第一指紋感測器偵測之值的子集。

【0080】 在704處，判定第一信號與同警示條件相關聯之所儲存資料是否相匹配。與警示條件相關聯之所儲存資料可為表示使用者之指紋中之一者的資料。因此，若使用者將該指紋與指紋感測器接觸，則過程700沿著「是」路徑進行至706。

【0081】 在706處，產生警示。警示可由圖4所示之警示模組420產生。警示可通知權責機關使用者尋求幫助且可防止系統完成任何命令。

【0082】 然而，若指紋並非「警示」手指之指紋，則過程700沿著「否」路徑進行至708。在708處，判定第一信號與第一所儲存資料是否相匹配。第一所儲存資料可表示使用者之指紋中之一者。對第一信號與所儲存資料相匹配的判定可藉由圖1所示之指紋辨識模組120在生物特徵感測器上實行。或者，此比較可諸如藉由伺服器310之生物特徵認證模組312在另一運算裝置上實行。

【0083】 若信號與所儲存資料不匹配，則指紋並非經認證之指紋且過程700沿著過程結束之「否」路徑進行且系統不產生命令。然而，若第一資料與所儲存資料確實匹配，則判定指紋為經認證之指紋且接著過程700沿著「是」路徑進行至710。

【0084】 在710處，自指紋感測器接收表示第二指紋之第二信號。可藉由在704處接收第一信號之相同的指紋感測器或藉由不同的指紋感測器接收第二信

號。例如，在704處接收之第一信號可自第一生物特徵感測器202接收，且在710處接收之第二信號可自如圖2所示之第二生物特徵感測器204接收。

【0085】 在712處，判定第二信號與同警示條件相關聯之資料是否相匹配。例如，即使使用者呈現之第一手指並非「警示」手指，但使用者稍後在過程中仍可藉由呈現「警示」手指而觸發警示。若將第二信號識別為對應於啟動警示條件之指紋，則過程700沿著「是」路徑進行至706，在706處如先前所描述產生警示。

【0086】 現在進行至圖7B，在714處，判定第二信號與第二所儲存資料是否相匹配。因此判定第二信號與第二經認證之指紋是否相匹配。如上文所描述，自對感測指紋之指紋感測器回應接收的資料與表示經認證之指紋之所儲存資料的比較可藉由生物特徵感測器100上之指紋辨識模組120或伺服器310上之生物特徵認證模組312進行比較。

【0087】 若第二信號與第二所儲存資料不匹配，則過程700沿著「否」路徑進行並結束而不認證命令。因此，在此實例中，必須呈現兩個指紋且每一指紋必須為經認證之指紋。在實施方案中之許多中，兩個指紋將對應於使用者之不同手指。藉由多次呈現同一指紋來產生命令亦為可能的。此外，經認證之指紋的序列可包括來自多個個體之指紋。例如，可能需要使用者之指紋及系統管理者之指紋兩者來產生刪除帳戶之命令。儘管過程700僅描述對應於兩個指紋之兩個信號，但類似的過程可以三個或更多個信號實施。

【0088】 若判定第二信號與第二所儲存資料匹配，則過程700沿著「是」路徑進行至716。在716處，識別第一信號及第二信號之時間順序。時間順序可為第一信號先於第二信號，第二信號先於第一信號，或兩個信號同時或實質上同時被接收。時間順序可為雙因素鑑別之第二因素，必須亦滿足該第二因素以便認證命令之實施。因此，僅呈現正確的手指給指紋感測器是不夠的，該等手指

必須亦以正確的順序呈現。此提供額外安全性，因為即使罪惡的使用者以某種方式控制了經認證之使用者的指紋，罪惡之使用者亦必須知道時間順序。

【0089】 在718處，判定時間順序與預定義時間順序是否相匹配。若否，則過程700沿著「否」路徑進行並結束。若時間順序相匹配，則過程700沿著「是」路徑進行至720。

【0090】 在720處，回應於以正確的時間順序接收正確的生物特徵輸入而產生命令。命令可包括按照慣例由運算裝置實施之任何命令，諸如解密資料，以信號示意機械鎖打開等。在一些實施方案中，命令可與表示生物特徵身分之軟體符記相關。軟體符記向接受者傳達藉由生物特徵技術對由軟體符記表示之使用者身分進行了驗證。命令可包括將軟體符記釋放至另一運算裝置。命令亦可包括授權運算裝置將軟體符記插入至區塊鏈檔案之公開帳簿中。

帳戶重置

【0091】 若使用者因為意外而丟失了他或她的指紋，則若存在用於收回對由生物特徵資料保護之帳戶及資訊之存取的機制將為有益的。重置帳戶可自帳戶清除生物特徵鑑別特徵並返回對先前使用之技術的帳戶存取，諸如密碼。在一個實施方案中，可藉由第二類型之生物特徵資料校驗使用者之身分。例如，使用者可提供虹膜掃描以獲得對他或她的指紋掃描之所儲存記錄的存取並使用所儲存之指紋掃描來重置帳戶。

【0092】 在另一實施方案中，第二類型之生物特徵資料可為使用者之基因資訊。因此，諸如藉由頰拭子自使用者獲得之去氧核糖核苷(DNA)序列可與使用者之帳戶關聯地儲存。可以電子方式儲存使用者之DNA之一部分的序列。其可例如與使用者之主指紋記錄412關聯地儲存。或者，來自使用者之組織之含有DNA的樣本(諸如頰拭子)可經儲存且在需要時定序以重置對帳戶之存取。

【0093】 為了在重置帳戶時提供額外安全性，使用者可提供第二類型之生物

特徵資料且亦提供第二因素，諸如指紋用以登錄帳戶之序列。因此，若藉由使用者呈現他的右手小拇指、左手小拇指及接著右手中指之指紋來存取儲存使用者之密碼中之許多的帳戶，則他可將該順序傳達給伺服器310或維護他的主指紋記錄412之其他系統，且若該順序成功地存取了他的帳戶，則帳戶將經重置。可藉由要求維護伺服器310之實體的員工授權重置來提供帳戶重置期間的進一步安全性。

安全性

【0094】 可藉由將存取限於僅提供了有效的生物特徵身分之使用者來保護系統或運算裝置。此可例如藉由要求存取網站伺服器之每一運算裝置藉由向網站伺服器提交之每一命令提供生物特徵符記來實施。因此，不提供生物特徵符記之裝置將不能存取網站伺服器且對網站伺服器之所有存取將可追蹤至已知的生物特徵身分。此可阻止駭客試圖存取網站伺服器，因為任何存取需要連結至實際個人之生物特徵的符記。

【0095】 藉由需要生物特徵符記以進行存取來限制存取可創建網站或域，其中存在每一存取成員為已知的環境。此可創建受生物特徵符記保護之網路。可由生物特徵符記保護之網路的實例為虛擬私人網路(VPN)。可藉由經由使用專用連結、虛擬隧道協定或基於生物特徵符記之流量加密建立虛擬點對點連接來創建VPN。

【0096】 若不提供適當符記之運算裝置試圖訪問網站、網站伺服器、域等，則可藉由以低階電腦碼發送大量無用資料至該運算裝置而強迫運算裝置離線。例如，可向不提供正確符記之運算裝置發送機器碼或機器語言中之隨機命令。作為進一步實例，可向試圖存取而不提供生物特徵鑑別之運算裝置發送包括組合語言指令之靜態。

區塊鏈整合

【0097】 經由生物特徵證明身分對於區塊鏈或在無中央當局確認使用者身分的情況下發揮作用之其他同級系統可特別有用。區塊鏈可包括一系列資料區塊，該等區塊包括碼，諸如保密散列或核對和，其與該系列中之先前區塊的內容可為編碼一致的。在一些情況下，判定產生相同的完整性碼之區塊的多個不同集合可為不可解決的、運算極度複雜的，或另外工作量足夠密集的以挫敗竄改區塊鏈之內容同時維護完整性碼之自身一致性的嘗試。修改區塊鏈之使用者(諸如加密貨幣之買家或賣家或智慧合約之參與者)之身分的證明可藉由添加生物特徵資料或藉由表示生物特徵身分之符記而記錄在區塊鏈自身中。

【0098】 在各種系統中，多方可使用基於區塊鏈之檔案或帳簿來維護事件、交易或其他更新之防篡改記錄。在一些情況下，區塊鏈可在藉由不信賴之一方，例如已存取區塊鏈而不提供生物特徵符記之一方對區塊鏈做出改變之後登記竄改。因此，該等方可個別地校驗由其他方進行之更新為有效的且與區塊鏈之先前的資料區塊為編碼一致的。即使一方缺乏用作參考之區塊鏈的歸檔版本，完整性碼之自身一致性亦允許校驗對區塊鏈之更新。當對區塊鏈中之一或多個資料區塊的重寫入在完整性輸出與區塊鏈中之區塊之資料區塊內容中不引入編碼不一致性時，重寫入可表徵為保留區塊鏈之有效性。

【0099】 區塊鏈可由完整性碼保護。當提供特定資料作為完整性碼之輸入時，完整性碼可產生特定完整性輸出。在一些情況下，當向完整性碼提供與特定資料不同之資料作為輸入時，完整性碼可產生不同的完整性輸出。在實例情形中，儲存由來自資料區塊之特定輸入資料產生的完整性碼之完整性輸出且稍後改變資料區塊。若將改變後之資料作為輸入提供至完整性碼，則完整性碼可產生不同的或另外與所儲存之完整性輸出編碼不一致之完整性輸出。因此，在此實例情形中可偵測改變。完整性碼可整體或部分基於生物特徵資料之表示，諸如表示使用者之指紋之掃描的資料或表示使用者之生物特徵身分的符記。

【0100】 區塊鏈可包括一系列區塊，其中該系列中之每一後續區塊保持前一區塊之完整性輸出。該系列可形成區塊鏈，其中每一後續區塊保持自緊接之前的區塊中存在之資料產生的完整性輸出。因此，若區塊改變，則可偵測到與儲存在後續區塊中之完整性輸出的編碼不一致性。由於完整性輸出為區塊中之所儲存資料的一部分，因此亦可經由編碼不一致性偵測對完整性輸出本身之改變。完整性碼之此自身一致性可用以關於隱秘竄改保護區塊鏈。

【0101】 當由完整性碼保護時，防篡改改變可虛擬地包括任何改變，對於該改變可偵測到用於區塊鏈之完整性碼之完整性輸出與區塊鏈內之資料之間的編碼不一致性。例如，區塊鏈之區塊中的資料可散列化，貫穿核對和，或應用另一完整性碼。若稍後發現區塊中之資料與散列、核對和或其他完整性碼之完整性輸出衝突，則可將改變識別為防篡改的。當當前在區塊中之資料不產生與之前在將完整性碼應用於當前在區塊中之資料時獲得的完整性輸出相同或等效的完整性輸出時，衝突可發生。當對區塊做出改變且之後不可偵測到與完整性碼之先前儲存之完整性輸出的編碼不一致性時，該改變可為非防篡改的。在一些情況下，可藉由以第二區塊取代第一區塊來實施非防篡改重寫入，第二區塊具有產生相同(或等效)完整性輸出之不同資料內容。

【0102】 區塊鏈之一個用途為實施智慧合約。智慧合約可表示為區塊鏈中之個別記錄的內容，其可包括發送者與接收者之間的合約義務或權利。智慧合約可在個別使用者、合作夥伴、企業或公司之間。智慧合約中之參與者之身分的確認可藉由使用生物特徵識別符來記錄。例如，表示智慧合約之一方之生物特徵身分的符記可包括在實施智慧合約之區塊鏈中。智慧合約可涉及軟體碼之循環執行。智慧合約內之軟體碼可包括在滿足某些條件時可經執行之軟體碼。

【0103】 用於出於多個不同目的中之任一者創建區塊鏈之系統的一個實例為以太坊。以太坊為可用以創建加密貨幣、智慧合約或可使用區塊鏈之任何其他

應用程式的分佈式公共區塊鏈網路。本文中描述之用於在區塊鏈上實施的技術中之任一者可使用以太坊或其他類似技術實施。

說明性應用程式

【0104】 本文中描述之硬體及技術可在許多不同情形中應用。例如，生物特徵感測器可用以實施門之實體鎖、機動車、保險箱等。使用詳細電容讀數以確認活組織之存在及基於呈現指紋之順序的雙因素鑑別相對於習知指紋感測器增加了安全性。此等優點可在無網路連接之情況下僅藉由生物特徵感測器自身中包括之系統實施。

【0105】 若生物特徵感測器連接至網路，則其可與伺服器(諸如圖3中介紹之伺服器310)通信，使得伺服器可提供與使用者之帳戶相關聯的鑑別服務及資料。例如，實施有指紋感測器且藉由藍芽連接至行動電話之汽車或轎車鑰匙可用以對多個不同汽車中之一者(諸如轎車共用車輛)解鎖。指紋感測器可確認操作轎車鑰匙之使用者的身分且藉由行動電話經由網路連接存取之伺服器或其他運算裝置可向轎車共用車輛之操作者提供支付資訊。此實施方案同樣可適用於自駕車輛。

【0106】 對醫療資訊及藥物之存取可由如本文中描述之生物特徵安全性控制。例如，在醫療提供者辦公室存取之醫療資訊或在藥房所填之處方可部分經由使用者經由諸如本文中描述之生物特徵感測器之裝置呈現生物特徵資料來認證。

【0107】 生物特徵鑑別亦可用以存取腦機介面(BMI)。BMI為增強或連線之大腦與外部裝置之間的直接通信路徑。BMI與神經協調作用之不同之處在於其允許雙向資訊流。BMI經常針對研究、映射、輔助、加強或修復人類認知或感官動作功能。BMI之一個用途可為向使用者提供與積極思維相關聯之腦波。與積極思維相關聯之腦波可包括當使用者處於γ波狀態下時產生之腦波。γ波為頻

率在25 Hz與100 Hz之間(通常大約40 Hz)的人類之神經振盪的型樣。BMI裝置可向使用者之大腦提供使大腦進入γ波狀態之信號。BMI裝置與使用者積極大腦之間的介面可由生物特徵感測器調節，使得使用者可控制向他或她的大腦提供之信號。

【0108】 使用者可回應於特定生物特徵輸入(諸如指紋組合)而使BMI裝置產生與積極思維(諸如γ波狀態)相關聯之信號。能夠直接控制大腦狀態可允許使用者抵制自我產生或外部施加之消極思維。外部施加之消極思維之一個可能來源可為人類與人工智慧(AI)之互動。如本文中所使用，與人類及其他動物顯示之天然智慧形成對比，人工智慧為由機器展示之智慧。在電腦科學中，將AI研究定義為學習「智慧型代理器」：感知其環境且採取行動之任何裝置，該等行動最大化其成功實現目標之機會。

實例實施例

【0109】 以下條款描述了用於實施本揭示內容中描述之特徵的多個可能實施例。本文中描述之各種實施例為非限制性的，來自任何給定實施例之每一特徵亦無需存在於另一實施例中。除非上下文另外清楚地指示，否則實施例中之任何兩個或更多個可組合在一起。如本文中所使用，在此文檔中，「或」意謂及/或。例如，「A或B」意謂A無B，B無A，或A及B。如本文中所使用，「包括」意謂包括所有列出特徵且可能包括未列出之其他特徵的添加。「基本上由……組成」意謂包括所列特徵及材料上不會影響所列特徵之基本及新穎特性的彼等額外特徵。「由……組成」僅意謂所列特徵，而將未列出之任何特徵排除在外。

【0110】 A：一種生物特徵識別裝置，其包括：一處理器；一指紋感測器，其經組態以回應於一指紋與該指紋感測器之接觸而產生脊部及谷部讀數之一景貌；一加密記憶體，其儲存與一字串相關聯之一加密值；至一運算裝置之一通

信連接；以及記憶體，其儲存指令，該等指令在由該處理器執行時使該處理器：接收該字串；判定該指紋經認證來存取該加密記憶體；解密該加密值以產生一值；以及提供該值至該運算裝置。

【0111】 B：如條款A之生物特徵識別裝置，其中該加密值為一加密密碼且該字串為一統一資源定位器(URL)或該加密值為一加密信用卡號碼且該字串為一信用卡之一名稱。

【0112】 C：如條款A或B之生物特徵識別裝置，其中該字串為該URL且接收該字串包括經由該通信連接自該運算裝置上之一網頁瀏覽器接收該URL。

【0113】 D：如條款A至C中任一項之生物特徵識別裝置，其進一步包括：一顯示器，其經組態以顯示該字串；以及一輸入裝置，其經組態以改變該顯示器上顯示之該字串。

【0114】 E：如條款D之生物特徵識別裝置，其中接收該字串包括偵測該顯示器中顯示之該字串。

【0115】 F：如條款A至E中任一項之生物特徵識別裝置，其進一步包括一第二指紋感測器，該第二指紋感測器經組態以回應於一第二指紋與該第二指紋感測器之接觸而產生脊部及谷部讀數之一第二景貌，該第二指紋與該第二指紋感測器之該接觸及該指紋與該指紋感測器之該接觸為同時的。

【0116】 G：如條款A至F中任一項之生物特徵識別裝置，其中該指紋感測器為一電容式指紋感測器且該等脊部及谷部讀數為電容讀數。

【0117】 H：如條款G之生物特徵識別裝置，其中該等指令經進一步組態以：比較脊部及谷部電容讀數之該景貌與活組織之一已知特性；以及判定該指紋係由活組織產生。

【0118】 I：如條款H之生物特徵識別裝置，其中活組織之該已知特性係基於指紋之脊部與谷部之間的濕度及/或溫度的差異。

【0119】 J：一種雙因素生物特徵識別之方法，其包括：自一或多個指紋感測器接收表示一第一指紋之一讀數的一第一信號及表示一第二指紋之一讀數的一第二信號；比較該第一信號與一第一所儲存資料；判定該第一信號與該第一所儲存資料相匹配；比較該第二信號與一第二所儲存資料；判定該第二信號與該第二所儲存資料相匹配；識別該第一信號及該第二信號之一時間順序；判定該時間順序與一預定義時間順序相匹配；以及產生一命令。

【0120】 K：如條款J之方法，其中該第一信號係自一第一指紋感測器接收且該第二信號係自一第二指紋感測器接收。

【0121】 L：如條款J或K之方法，其中該第一指紋與一第一整數相關聯，該第二指紋與一第二整數相關聯，且該命令與一數值相關聯，該數值為該第一整數後接該第二整數。

【0122】 M：如條款J至L中任一項之方法，其中該第一信號或該第二信號與同一警示條件相關聯之所儲存資料相匹配且產生該命令包括產生一警示。

【0123】 N：如條款J至M中任一項之方法，其中該命令授權一運算裝置釋放一軟體符記。

【0124】 O：如條款J至N中任一項之方法，其中該命令授權一運算裝置將一軟體符記插入至一區塊鏈檔案之一公開帳簿中。

【0125】 P：一種系統，其包括：一或多個處理器；一記憶體；主指紋記錄，該等主指紋記錄含有複數個指紋型樣之表示；一使用者介面模組，其經組態以產生用於一使用者介面之指令，該使用者介面包括至複數個服務提供者之連結，每一連結與兩個或更多個不同指紋型樣之一組合相關聯；一指紋加密/解密模組，其經組態以解密表示一第一指紋型樣及一第二指紋型樣之加密資料，以產生一未加密之第一指紋型樣及一未加密之第二指紋型樣；一生物特徵認證模組，其經組態以將該第一未加密之指紋型樣與該等主指紋記錄中之一第一所

保存指紋型樣相匹配，將該第二未加密之指紋型樣與該等主指紋記錄中之一第二所保存指紋型樣相匹配；以及產生存取與該複數個服務提供者中之一者相關聯的該等連結中之一者的一命令，該等連結中之該一者係基於該第一指紋型樣及該第二指紋型樣之一順序而選擇。

【0126】 Q：如條款P之系統，其中該等主指紋記錄針對一使用者含有表示與該使用者之十個手指對應之十個指紋型樣的資料。

【0127】 R：如條款P或Q之系統，其中該生物特徵認證模組經進一步組態以基於該第一指紋型樣及該第二指紋型樣判定一使用者之一身分，其中該身分為與該使用者之一或多個公眾已知之特性相關聯的一公開身分，或其中該身分為與一使用者之一公眾已知之特性無關聯但與一或多個電子帳戶相關聯的一匿名身分。

【0128】 S：如條款R之系統，其中該指紋加密/解密模組經進一步組態以藉由使用與該使用者之該身分相關聯的一合成地產生之任意指紋型樣來解密表示該第一指紋型樣之該加密資料。

【0129】 T：如條款P至S中任一項之系統，其進一步包括一符記化模組，該符記化模組經組態以提供一生物特徵符記至該複數個服務提供者中之該一者，該生物特徵符記基於該第一指紋型樣及該第二指紋型樣而提供一使用者之一身分的證明。

總結

【0130】 除非本文中另有指示或明顯與上下文相抵觸，否則在描述本發明的上下文中(尤其在隨附申請專利範圍的上下文中)使用的術語「一」、「該」、「該等」以及類似指代應解釋為涵蓋單數形式與複數形式兩者。術語「基於」應解釋為涵蓋排他性及非排他性關係。例如，「A係基於B」意謂A至少部分基於B且可完全基於B。「大約」意謂變化多達參考數量、等級、值、數目、頻率、百分

比、尺寸、大小、量、重量或長度之10%、9%、8%、7%、6%、5%、4%、3%、2%、1%的數量、等級、值、數目、頻率、百分比、尺寸、大小、量、重量或長度。

【0131】 除非本文中另外指示或上下文另外清楚地反駁，否則本文中描述之所有方法可以任何合適的順序實行。除非另外主張，否則本文中提供之所有實例及例示性語言(例如，「諸如」)的使用僅意欲較佳地說明本發明且不對本發明之範疇施加限制。說明書中之語言不應解釋為指示任何非主張元素對於本發明之實踐為必要的。

【0132】 本文中揭示之本發明之替代元素或實施例的群不應解釋為限制。每一群成員可經參考且個別地或與群之其他成員或本文中發現之其他元素任意組合地進行主張。預期出於方便及/或專利性之理由，群之一或多個成員可包括在群中或自群刪除。當任何此包括或刪除發生時，認為說明書含有修改之群，因此實踐所附申請專利範圍中使用之所有馬庫西群之書面描述。

【0133】 本文中描述了某些實施例，包括發明者已知之用於執行本發明之最佳模式。當然，在閱讀以上描述後，對此等所描述之實施例的變化對一般熟習此項技術者而言將變得顯而易見。熟習此項技術者將知道如何在適當時採用此等變化，且本文中揭示之實施例可以除了具體描述以外之方式實踐。因此，本文所附之申請專利範圍中所述之標的的所有修改及等效物包括在本揭示內容之範疇內。此外，除非本文中另外指示或上下文另外清楚地反駁，否則本發明涵蓋所有可能變化中之上述元素的任何組合。

【0134】 儘管已按對結構特徵及/或方法動作特定之語言描述了標的，但應理解，所附申請專利範圍中定義之標的不必限於所描述之特定特徵或動作。更確切而言，按照實施申請專利範圍之說明性形式揭示特定特徵及動作。

附錄A

【0135】 為了量測活體中之電阻及電容，存在一種施加有限交流電，且自經過電位之振幅及相位角的變化求出電阻及電容之方法。此外，藉由此方法，求出暫態及常態之電阻及電容且獲得其在每一頻率下之值。暫態包括具有指數項之超越函數，指數項僅在常態下變成零，因此有可能使用對暫態求解之電腦程式獲得所有狀態。將有限交流電施加至人類皮膚持續三個循環，且量測其在每一頻率下之電阻及電容。

I. 總體論述

【0136】 存在使用直流電及交流電以量測人類皮膚之電阻及電容的方法。在使用交流電之方法中，通常已使用交流電橋執行量測。

【0137】 該橋之兩個分支與電阻器R_1及R_2串聯地耦接，分支中之一者與電阻器r_1及電容器c_1串聯地耦接，而活組織用於與電阻器r_2及電容器c_2串聯地耦接之第四分支。若分支之阻抗為z_1、z_2、z_3及z_4，則

$$\frac{z_1}{z_2} = \frac{z_3}{z_4}$$

在其處於平衡狀態時保持。因此，

$$z_1 = R_1$$

$$z_2 = R_2$$

$$z_3 = r_1 + \frac{1}{j\omega c_1}$$

$$z_4 = r_2 + \frac{1}{j\omega c_2}$$

根據此，

$$\frac{R_1}{R_2} = \frac{r_1}{r_2}$$

$$\frac{R_1}{R_2} = \frac{c_2}{c_1}$$

【0138】 與此方法形成對比，若將交流電Em sin (ωt + ϕ)(其中Em為交流電之振幅且ω為角頻率)施加至電阻器r及電容器c，從而將經過電位導向輸入電阻R之量測裝置，其中出現之電流及電位為I及v，則

$$E_m \sin \omega t = (R + r) i + \frac{1}{c} \int i dt$$

$$\omega E_m \cos \omega t = (R + r) \frac{di}{dt} + \frac{i}{c}$$

當 $\frac{di}{dt} = 0$ 時，若i為i_m，v為v_m，且t為t_m，則

$$\omega E_m \cos \omega t_m = \frac{i_m}{c}$$

$$i_m = \frac{v_m}{R}$$

根據此，

$$c = \frac{v_m}{\omega R E_m \cos \omega t_m}$$

或根據

$$(R + r) \frac{v}{R} + \frac{1}{Rc} \int v dt = E_m \sin \omega t$$

$$v = V_m \left\{ \sin (\omega t + \phi) - \sin \phi \varepsilon^{-\frac{t}{(R+r)c}} \right\}$$

此處，

$$V_m = \frac{RE_m}{\sqrt{(R+r)^2 + (\frac{1}{\omega c})^2}}$$

$$= \frac{RE_m}{R+r}\cos\phi$$

$$\tan\phi = \frac{1}{\omega(R+r)c}$$

且若 $\frac{dv}{dt} = 0$，則

$$\cos(\omega t_m + \phi) + \sin\phi \tan\phi \varepsilon^{-\omega t_m \tan\phi} = 0$$

且若根據此$\tan\phi = x$，則

$$x\sin\omega t_m - \cos\omega t_m = x^2\varepsilon^{-\omega t_m x}$$

且電腦可用以自ω及t_m求出x，則

$$\tan\phi = \frac{1}{\omega(R+r)c}$$

r可自c獲得，c自ω、R、E_m、V_m及ω及t_m獲得。換言之，此為暫態下之活體的電阻及電容。

【0139】　相比之下，如下獲得常態下之電阻及電容。由於常態為$t \approx \infty$，

$$v = V_m \sin(\omega t + \phi)$$

推斷自

$$v = V_m \left\{\sin(\omega t + \phi) - \sin\phi \varepsilon^{-\frac{t}{(R+r)c}}\right\}$$

因為陽極之值$\sin(\omega t + \phi) = 1$，

$$v = V_m$$

$$= \frac{RE_m}{R+r}\cos\phi$$

最大時，

$$\sin(\omega t + \phi) = 1$$

$$\omega t + \phi = \frac{n\pi}{2}$$

此外，當$E_m \sin \omega t = E_m$時，

$$\omega t = \frac{n\pi}{2}$$

因此，V_m與E_m之間的相位差為ϕ，且藉由自ϕ及V_m之值求出r。

$$\tan\phi = \frac{1}{\omega(R + r)c}$$

根據此獲得c。

【0140】 然而，當將此兩個進行比較時，後者僅適用於常態，且明顯不能處置暫態。前者為最初經開發以對暫態求解之等式，但此情況下包括t作為極限及無窮，因此其可對t為無窮之情況求解。由於t可為任何值，因此可想像可獲得暫態以及常態之答案。

【0141】 因此，將有限交流電施加至人類皮膚且在每一者為最大值時求出r及c。無常在一個循環期間發生，但在三個循環內幾乎始終存在常態，輕微無常包括在兩個循環中。

II.方法

【0142】 1. 電路：將有限交流電振盪器、人類皮膚，及量測裝置串聯地耦接。

【0143】 2.有限交流電振盪器：振盪器經設計以使用函數產生器輸出正弦波持續在一個與20個循環之間的僅期望數目個循環。可控制振幅及角頻率，且亦提供延遲裝置。

【0144】 3. 電極：將直徑為0.8 mm之銀線焊接至直徑為10 mm且厚0.3 mm之銀板，並將氯化銀用於表面。此等電極相隔40 mm黏附在箱形裝置上，該箱形裝置由長度40 mm、寬度100 mm及高度30 mm之塑膠製成。此經由受試者前臂

背面之皮膚上的3%Ringer氏溶液瓊脂而起電。

【0145】 4. 量測裝置：量測裝置用於數位記憶體，其中一個字元為50 ns至1 s，且包括具有1024個字元之兩個通道。使用示波器進行觀察，拍攝圖片，並使用印表機記錄值以用於分析。

III.結果

【0146】 藉由將半徑10-mm之Ag-AgCl電極置放在人類受試者之前臂背面且經由Ringer氏溶液瓊漿施加三個循環之有限交流電來進行實驗。量測經過電位作為5 KΩ之輸入電阻。將所施加電位及經過電位輸入至同一數位記憶體之通道1及2中且皆使用圖片及印表機列印出來。

【0147】 使用通道1之所施加電位來計算振幅E_m及角頻率ω。使用通道2量測最大v_1、v_2、v_3、v_4、v_5及v_6且求出其時間t_1、t_2、t_3、t_4、t_5及t_6。

【0148】 1. w = 1 ms

【0149】 此處w為數位記憶體中之字元。e = 2 V為通道1之滿刻度靈敏度，且v = 0.2 V為通道1之滿刻度靈敏度。

$$E_m = 1.46 \qquad (\text{V})$$

$$\omega = 2.78 \times 10 \qquad (\text{弧度/秒})$$

IV.觀察

【0150】 根據結果，當電流在運行時，在所有最大值下求出電阻及電容。

$$v = V_m \left\{ \sin(\omega t + \phi) - \sin\phi\, \varepsilon^{-\frac{t}{(R+r)c}} \right\}$$

為了使用此分析最大值，

$$f = \sin \omega t_m - x \cos \omega t_m$$

$$g = x^2 \varepsilon^{-\omega t_m x}$$

當輸入特定值x_1時，

f > g

或

f < g

根據此，

$$x_2 = x_1 + \frac{x_1}{m}$$

得到f > g

或

f < g

當此發生時，則

$$x_3 = x_2 + \frac{x_2}{m}$$

當此重複時，求出*x*使得

f≈g。

此*x*為

$$\tan\phi = \frac{1}{\omega(R+r)c}$$

且藉由此及

$$c = \frac{V_m}{\omega R E_m \cos\omega t_m}$$

求出*r*及*c*。然而，電腦包括程式，使得當輸入ω、E_m、v_m及t_m時，輸出*r*及*c*及1/2ω*c*。因此，在常態下，使用當t ≈ ∞時之同一程式來求出*r*及*c*，因此藉由將自實驗獲得之值原樣輸入至電腦中，輸出*r*及*c*之值而不管狀態如何。

【0151】　因此，自結果求出*r*及*c*且其值可用以在自暫態轉變為常態時求出其中的變化。

【0152】　因此，針對每一字元，在最大值下獲得所有電阻及電容值。在過去對人類皮膚中之交流電的研究中，Motokawa等人已在人類頭皮上使用交流電橋

得到阻抗圖，但其為常態，因為值係在平衡狀態使用交流電橋得到的。

【0153】 許多事情可以從目前的研究而非僅僅阻抗圖得到。讓我們提一下兩個或三個。

【0154】 每一字元中之第一最大值的值(實驗結果中為t_1)顯然為暫態且不同於之後的值。則問題在於是否存在管控隨時間值增長彼等值如何增長至最大值的某一法則，且儘管可想像某一類型的關係，但其並不適用於所有字元。第一t_1時之值顯然不同於之後的值。電阻之幾乎所有值均增長，且電容之趨勢相同。

【0155】 然而，當第二或第三改變時，把握關係未必一致。存在第一及第二傾向於增長，但對於t_3、t_4、t_5及t_6，在振盪方面接近固定值的許多情況，但亦存在與此偏離之情況。

【0156】 類似於過去的實驗，阻抗圖實驗涉及常態及暫態。

【0157】 電感亦在電阻上升時上升但非常接近地下降，因此看起來有建立弧之趨勢，但無顯著趨勢。

【0158】 存在與人類皮膚中之直流電相關的其他研究。Gildmeister認為電阻及電容之作用為反電動勢。Einthoven為第一個使用弦線電流計以相當準確地確定電流路徑的人，而Hozawa使用Pendel電流計及Balistik電流計以低至2 μs發現此。

【0159】 在使用直流電之此研究之後，存在在肌肉及神經上使用交流電之電流，量測係使用交流電橋進行的。使用具有交流電之電橋的量測方法存在許多誤差，因此開發了施加有限交流電之方法且其所施加電位及活體之經過電位用以主要使用振幅之變化及相位角之偏差來量測其電阻及電容。此等方法使得可能量測交流電暫態現象之電阻及電容，其可使用交流電橋進行量測。自電腦分析可同樣適用於常態之理論基礎開始，目前研究將此應用於人類皮膚，且獲得預期結果。本文中已對此等進行了報告。

V. 結論

【0160】 直流電及交流電已用於量測人類皮膚之電阻及電容，按照慣例已使用交流電，在交流電之情況下，涉及已知電阻輸入至之第二分支，使用第三分支之可變的串聯電阻及電容，及第四分支之活體以自其平衡狀態求出活體之電阻及電容。此為常態。

【0161】 相比之下，已開發藉由施加有限交流電及查看其振幅及相位角來求出活體之電阻及電容的方法。在此情況下，獲得暫態及常態現象，且藉由對包括指數函數之超越函數方程求解，電腦可用以求出暫態之電阻及電容。相比之下，常態中之指數項為零，從而得到可使用一般方法求解之代數方程。即使將呈現常態之大時間值插入暫態方程中，電腦亦可使用相同方法求出值。

【0162】 因此，將呈現常態之三個循環應用於人類皮膚，且電腦用以自六個最大值求出暫態及常態的所有電阻及電容。

【符號說明】

100	生物特徵感測器
102	感測墊
104	處理器
106	顯示器
108	輸入裝置
110	記憶體
112	加密記憶體
114	通信硬體
116	通信連接
118	外部運算裝置
120	指紋辨識模組

122	加密/解密模組
124	記錄產生模組
200	示出說明性UI之圖式
202	第一生物特徵感測器
204	第二生物特徵感測器
206	左手
208	右手
300	網路環境
302	生物特徵感測器
304(A)	第一運算裝置
304(B)	運算裝置
304(C)	第二運算裝置
306	通信連接
308	網路
310	伺服器
312	生物特徵認證模組
314	網站伺服器
400	示出伺服器內之組件的說明性方塊圖
402	處理器
404	記憶體
406	加密記憶體
408	網路連接
410	指紋加密/解密模組
412	主指紋記錄

414 使用者介面(UI)模組

416 所儲存資料提供模組

418 符記化模組

420 警示模組

500 使用者介面(UI)

502 第一連結

504 數字

600 使用生物特徵鑑別來擷取密碼之說明性過程

602 步驟

604 步驟

606 步驟

608 步驟

610 步驟

612 步驟

614 步驟

616 步驟

618 步驟

620 步驟

700 使用雙因素生物特徵識別以產生命令之說明性過程

702 步驟

704 步驟

706 步驟

708 步驟

710 步驟

712 步驟

714 步驟

716 步驟

718 步驟

720 步驟

201837764

【發明摘要】

【中文發明名稱】生物特徵感測器

【英文發明名稱】BIOMETRIC SENSOR

【中文】

一種生物特徵識別裝置可用以保護密碼及其他有價值之資訊。在一個實施方案中，該生物特徵識別裝置可為一電容式指紋感測器。電容讀數可用以識別一指紋之脊部及谷部且判定與該指紋感測器接觸之一物件是否為活組織。可藉由辨識生物特徵輸入之真實性及提供該等生物特徵輸入之一特定組合或序列而實施雙因素識別。提供一使用者介面，其中生物特徵輸入之序列與命令相關聯。一使用者可藉由提供一預定指紋序列至一指紋掃描儀而指示一命令。

【英文】

A biometric identification device may be used to secure passwords and other valuable information. In one implementation, the biometric identification device may be a capacitive fingerprint sensor. Capacitive readings may be used to identify the ridges and valleys of a fingerprint and determine if an object contacting the fingerprint sensor is living tissue. Two- factor identification may be implemented by recognizing the authenticity of biometric inputs and a specific combination or sequence in which the biometric inputs are provided. A user interface is provided in which sequences of biometric inputs are associated with commands. A user may indicate a command by providing a predetermined sequence of fingerprints to a fingerprint scanner.

【指定代表圖】圖1

【代表圖之符號簡單說明】

100　生物特徵感測器

102　感測墊

104 處理器

106 顯示器

108 輸入裝置

110 記憶體

112 加密記憶體

114 通信硬體

116 通信連接

118 外部運算裝置

120 指紋辨識模組

122 加密/解密模組

124 記錄產生模組

【發明申請專利範圍】

【第1項】 一種生物特徵識別裝置，其包括：

一處理器；

一指紋感測器，其經組態以回應於一指紋與該指紋感測器之接觸而產生脊部及谷部讀數之一景貌；

一加密記憶體，其儲存與一字串相關聯之一加密值；

至一運算裝置之一通信連接；以及

記憶體，其儲存指令，該等指令在由該處理器執行時使該處理器：

接收該字串；

判定該指紋經認證來存取該加密記憶體；

解密該加密值以產生一值；以及

提供該值至該運算裝置。

【第2項】 如請求項1之生物特徵識別裝置，其中該加密值為一加密密碼且該字串為一統一資源定位器(URL)或該加密值為一加密信用卡號碼且該字串為一信用卡之一名稱。

【第3項】 如請求項1之生物特徵識別裝置，其中該字串為該URL且接收該字串包括經由該通信連接自該運算裝置上之一網頁瀏覽器接收該URL。

【第4項】 如請求項1之生物特徵識別裝置，其進一步包括：

一顯示器，其經組態以顯示該字串；以及

一輸入裝置，其經組態以改變該顯示器上顯示之該字串。

【第5項】 如請求項4之生物特徵識別裝置，其中接收該字串包括偵測該顯示器中顯示之該字串。

【第6項】 如請求項1之生物特徵識別裝置，其進一步包括一第二指紋感測器，該第二指紋感測器經組態以回應於一第二指紋與該第二指紋感測器之

接觸而產生脊部及谷部讀數之一第二景貌，該第二指紋與該第二指紋感測器之該接觸及該指紋與該指紋感測器之該接觸為同時的。

【第7項】 如請求項1之生物特徵識別裝置，其中該指紋感測器為一電容式指紋感測器且該等脊部及谷部讀數為電容讀數。

【第8項】 如請求項7之生物特徵識別裝置，其中該等指令經進一步組態以：

比較脊部及谷部電容讀數之該景貌與活組織之一已知特性；以及

判定該指紋係由活組織產生。

【第9項】 如請求項8之生物特徵識別裝置，其中活組織之該已知特性係基於指紋之脊部與谷部之間的濕度及/或溫度的差異。

【第10項】一種雙因素生物特徵識別之方法，其包括：

自一或多個指紋感測器接收表示一第一指紋之一讀數的一第一信號及表示一第二指紋之一讀數的一第二信號；

比較該第一信號與一第一所儲存資料；

判定該第一信號與該第一所儲存資料相匹配；

比較該第二信號與一第二所儲存資料；

判定該第二信號與該第二所儲存資料相匹配；

識別該第一信號及該第二信號之一時間順序；

判定該時間順序與一預定義時間順序相匹配；以及

產生一命令。

【第11項】如請求項10之方法，其中該第一信號係自一第一指紋感測器接收且該第二信號係自一第二指紋感測器接收。

【第12項】如請求項10之方法，其中該第一指紋與一第一整數相關聯，該第二指紋與一第二整數相關聯，且該命令與一數值相關聯，該數值為該第一整數後接該第二整數。

【第13項】如請求項10之方法，其中該第一信號或該第二信號與一警示條件所相關聯之所儲存資料相匹配，且該產生該命令包括產生一警示。

【第14項】如請求項10之方法，其中該命令授權一運算裝置釋放一軟體符記。

【第15項】如請求項10之方法，其中該命令授權一運算裝置將一軟體符記插入至一區塊鏈檔案之一公開帳簿中。

【第16項】一種系統，其包括：

一或多個處理器；

一記憶體；

主指紋記錄，該等主指紋記錄含有複數個指紋型樣之表示；

一使用者介面模組，其經組態以產生用於一使用者介面之指令，該使用者介面包括至複數個服務提供者之連結，每一連結與兩個或更多個不同指紋型樣之一組合相關聯；

一指紋加密/解密模組，其經組態以解密表示一第一指紋型樣及一第二指紋型樣之加密資料，以產生一未加密之第一指紋型樣及一未加密之第二指紋型樣；

一生物特徵認證模組，其經組態以將該第一未加密之指紋型樣與該等主指紋記錄中之一第一所保存指紋型樣相匹配，將該第二未加密之指紋型樣與該等主指紋記錄中之一第二所保存指紋型樣相匹配；以及

產生存取與該複數個服務提供者中之一者相關聯的該等連結中之一者的一命令，該等連結中之該一者係基於該第一指紋型樣及該第二指紋型樣之一順序而選擇。

【第17項】如請求項16之系統，其中該等主指紋記錄針對一使用者含有表示與該使用者之十個手指對應之十個指紋型樣的資料。

【第18項】如請求項16之系統，其中該生物特徵認證模組經進一步組態以基於

該第一指紋型樣及該第二指紋型樣判定一使用者之一身分，

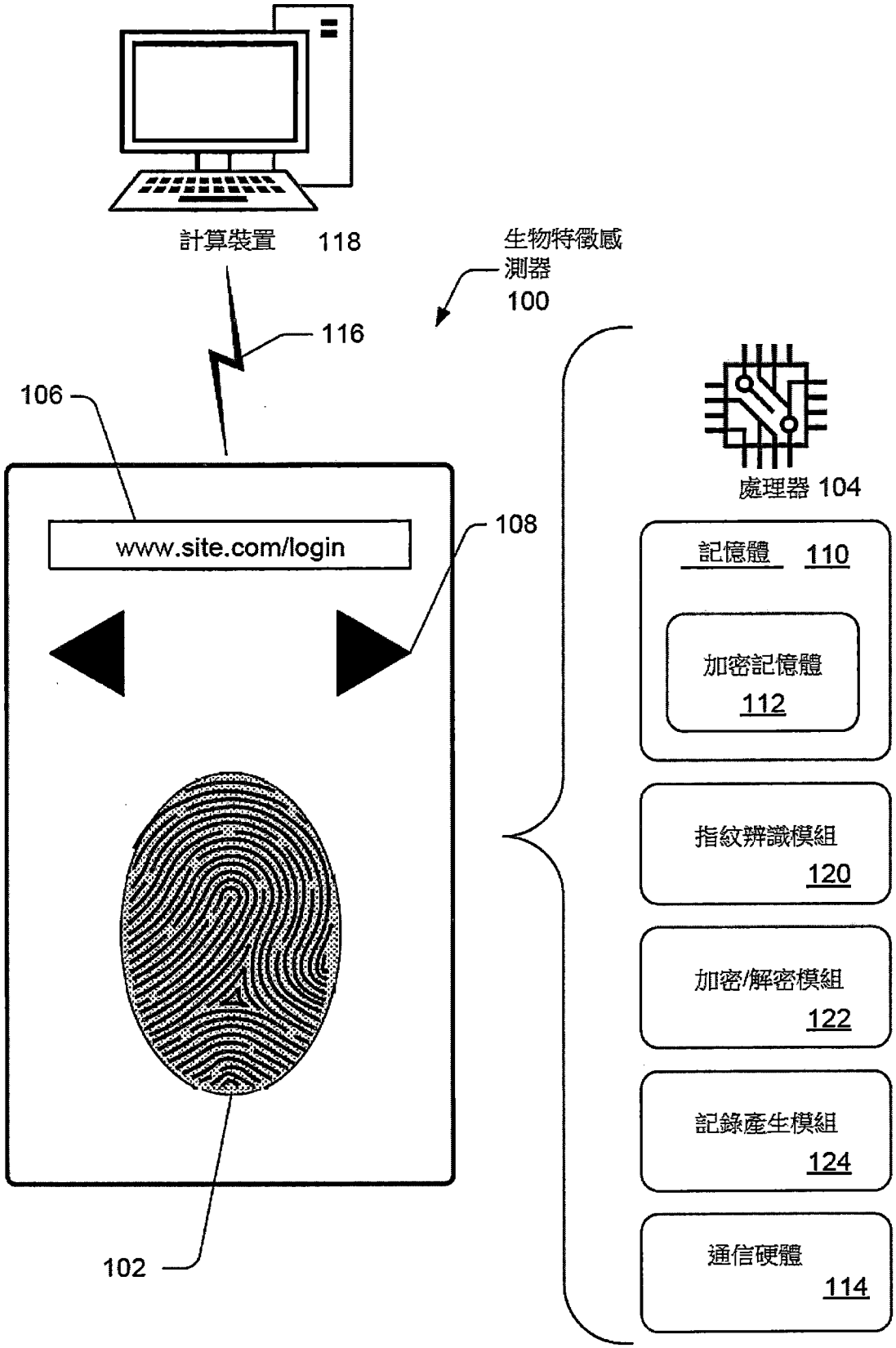
其中該身分為與該使用者之一或多個公眾已知之特性相關聯的一公開身分，或

其中該身分為與一使用者之一公眾已知之特性無關聯但與一或多個電子帳戶相關聯的一匿名身分。

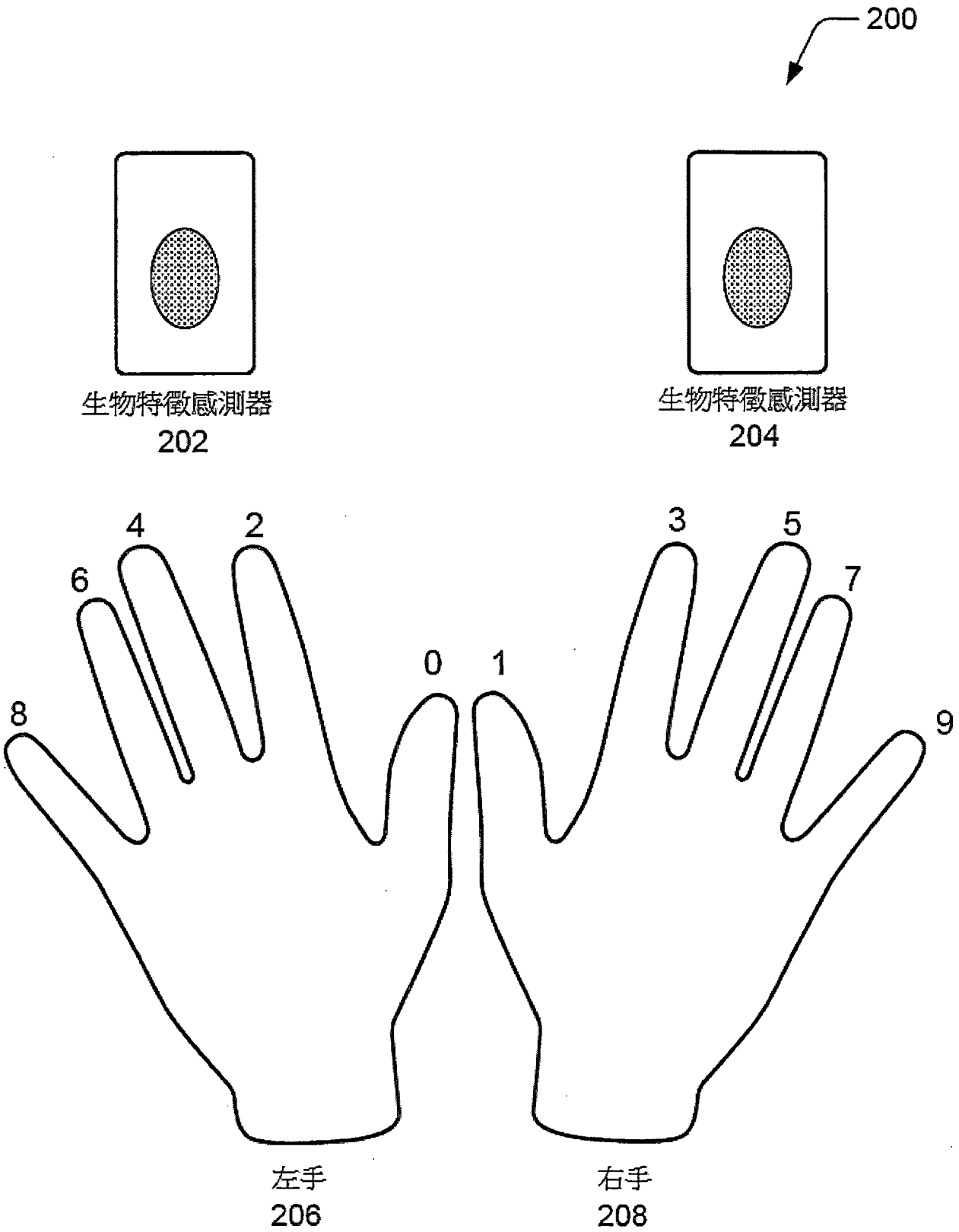
【第19項】如請求項18之系統，其中該指紋加密/解密模組經進一步組態以藉由使用與該使用者之該身分相關聯的一合成地產生之任意指紋型樣來解密表示該第一指紋型樣之該加密資料。

【第20項】如請求項16之系統，其進一步包括一符記化模組，該符記化模組經組態以提供一生物特徵符記至該複數個服務提供者中之該一者，該生物特徵符記基於該第一指紋型樣及該第二指紋型樣而提供一使用者之一身分的證明。

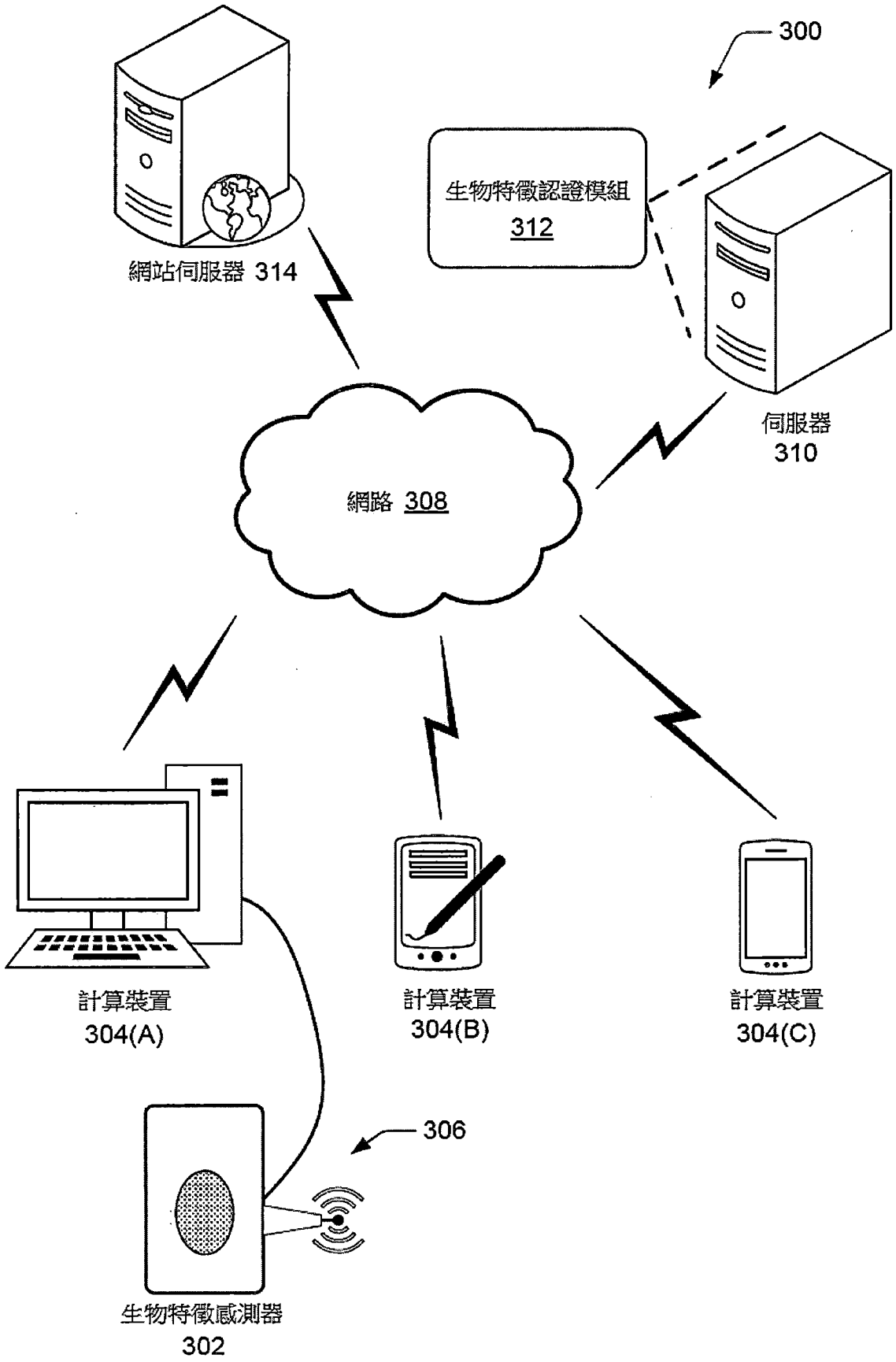
【發明圖式】


計算裝置 118
生物特徵感測器 100
116
106
www.site.com/login
108
102
處理器 104
記憶體 110
加密記憶體 112
指紋辨識模組 120
加密/解密模組 122
記錄產生模組 124
通信硬體 114

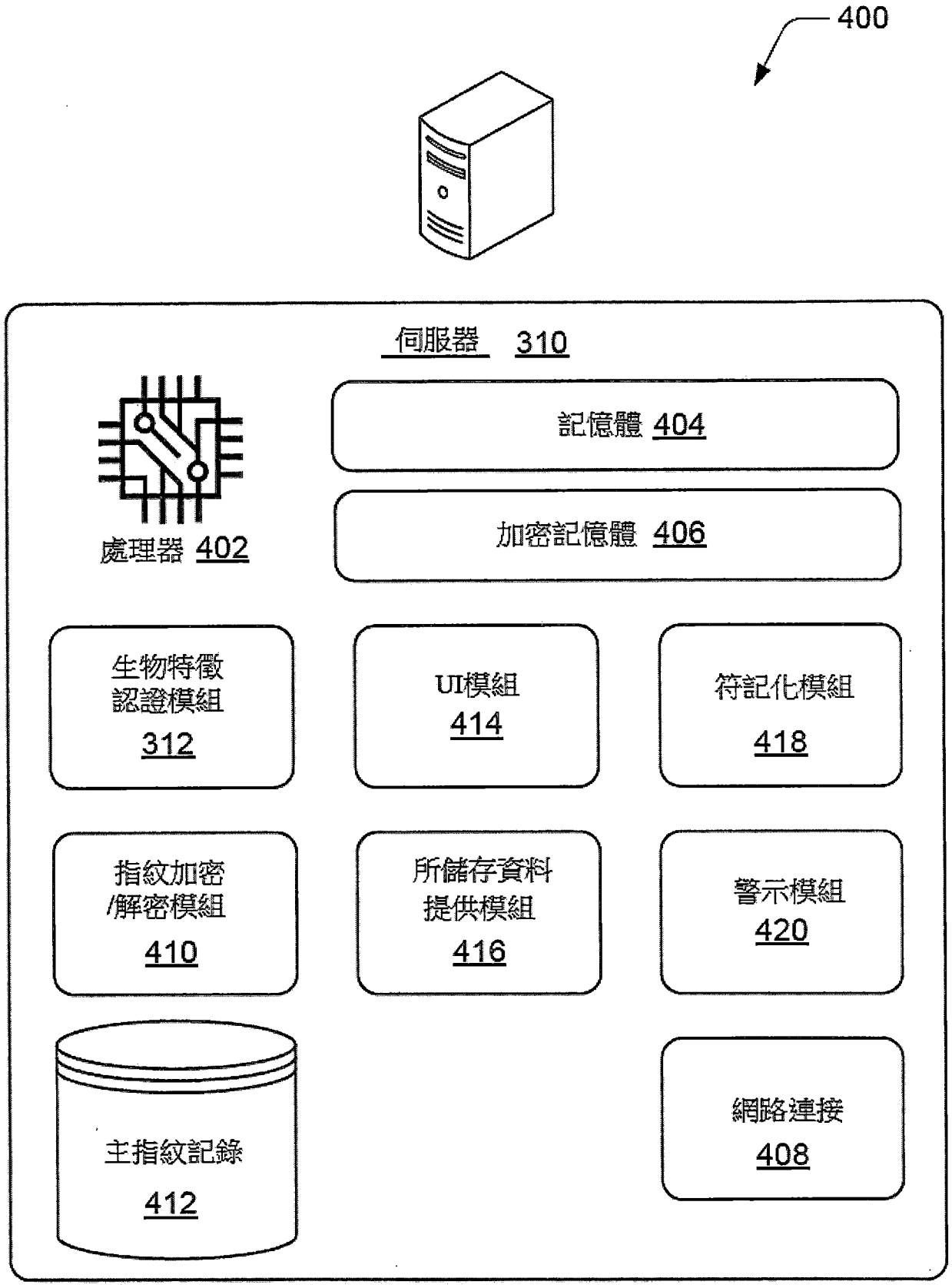
【圖 1】



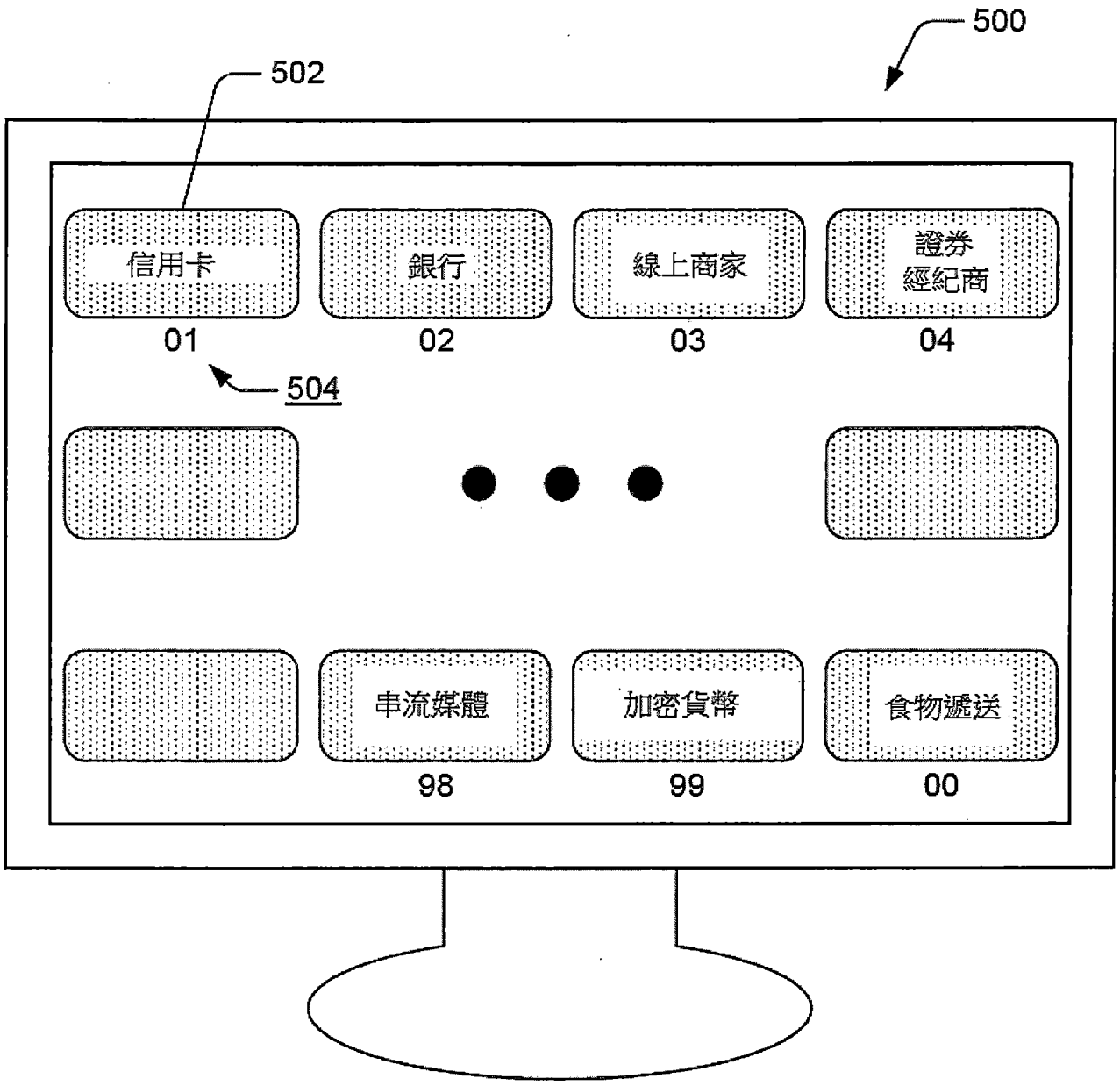
【圖 2】


300
生物特徵認證模組
312
網站伺服器 314
伺服器
310
網路 308
計算裝置
304(A)
計算裝置
304(B)
計算裝置
304(C)
306
生物特徵感測器
302

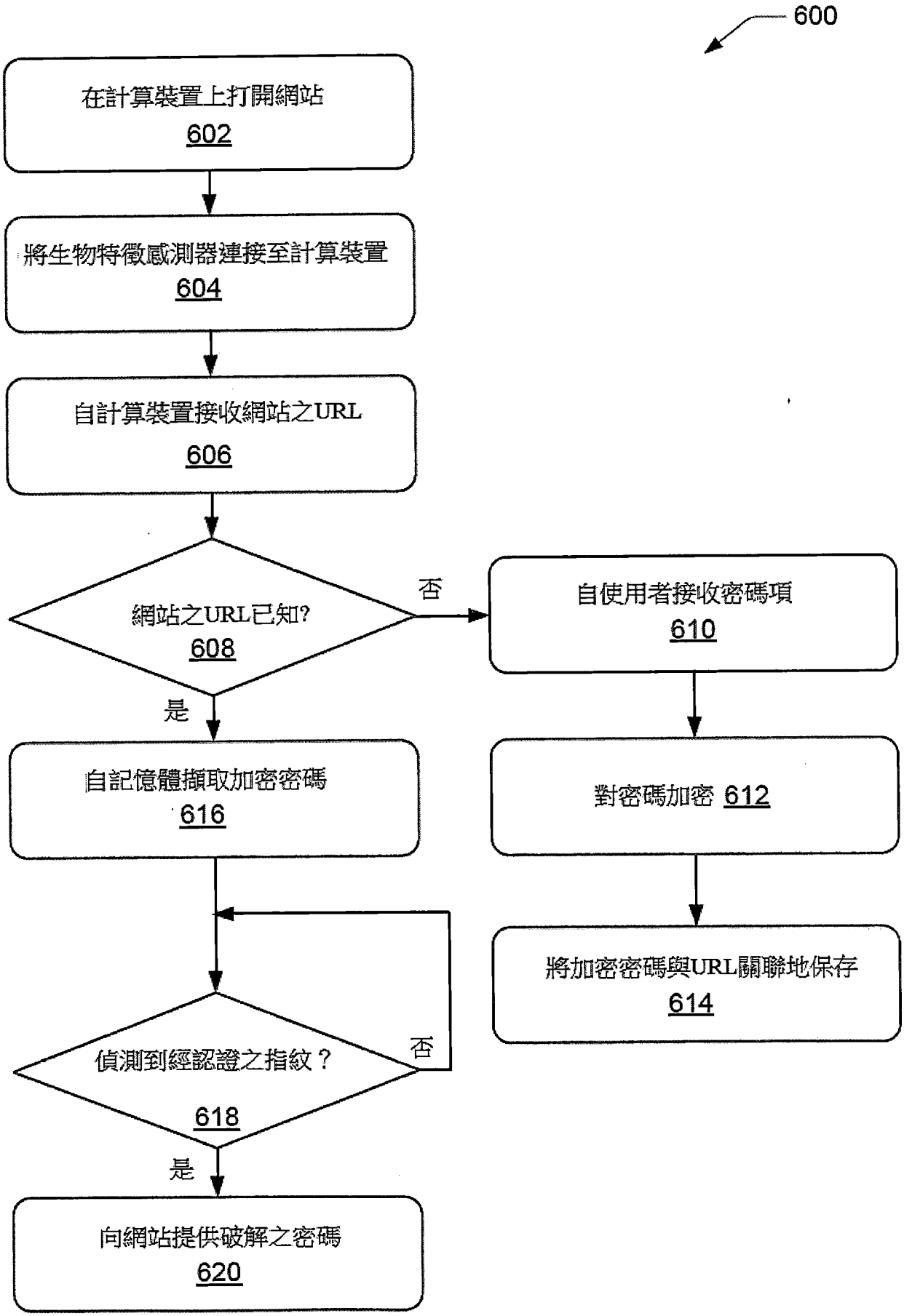
【圖 3】


400
伺服器 310
記憶體 404
加密記憶體 406
處理器 402
生物特徵
認證模組
312
UI模組
414
符記化模組
418
指紋加密
/解密模組
410
所儲存資料
提供模組
416
警示模組
420
主指紋記錄
412
網路連接
408

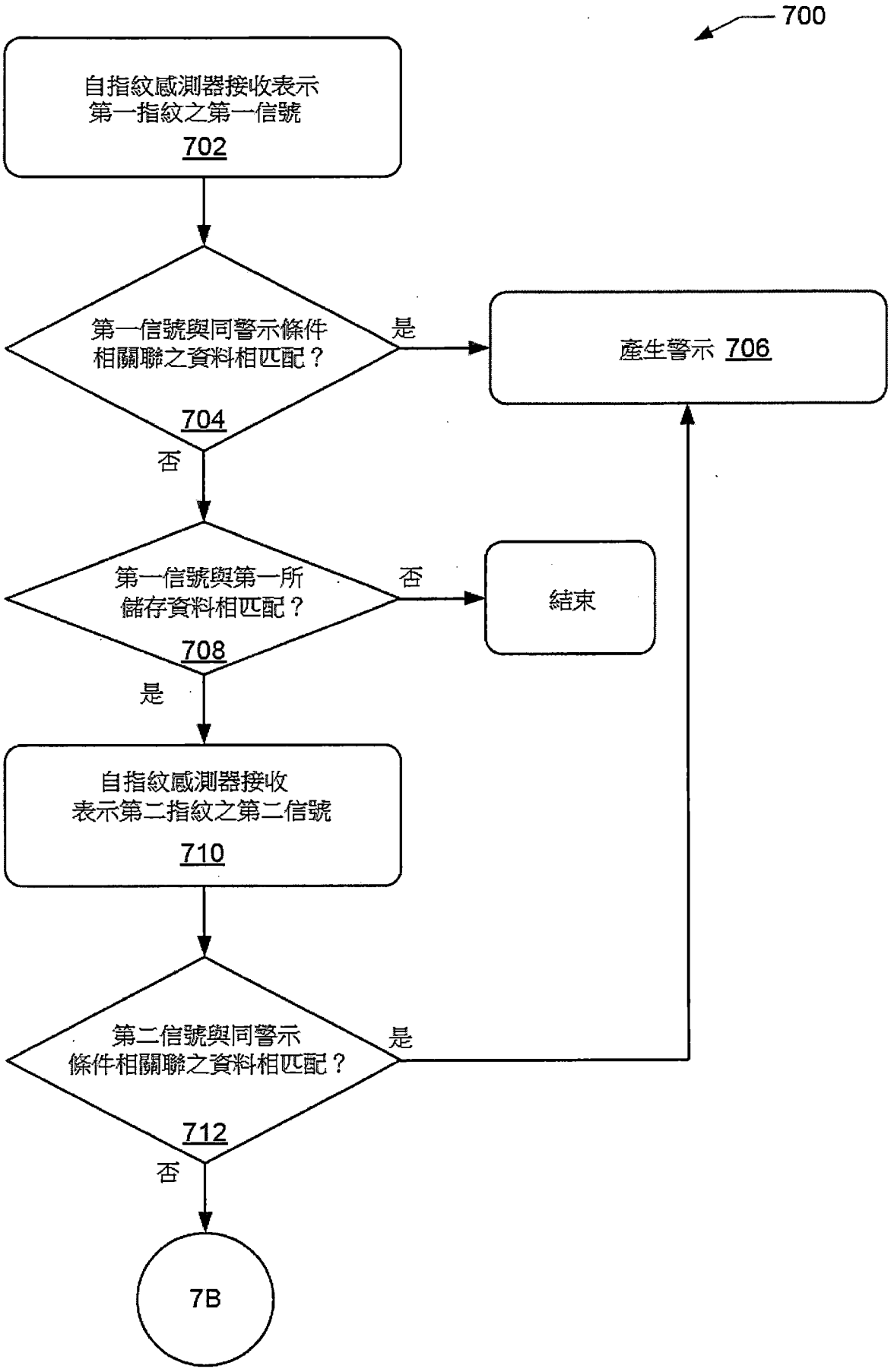
【圖 4】



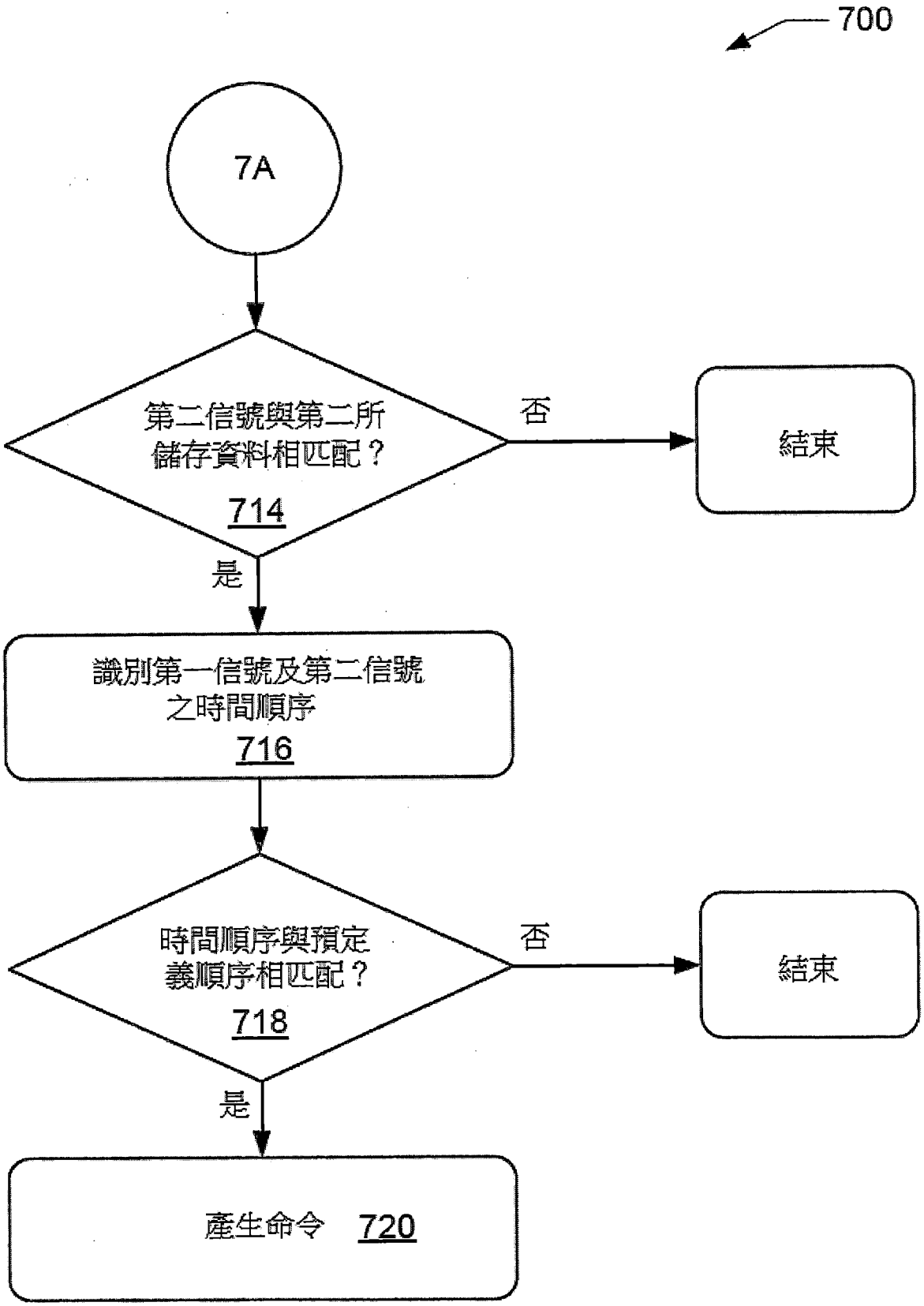
【圖 5】


600
在計算裝置上打開網站
602
將生物特徵感測器連接至計算裝置
604
自計算裝置接收網站之URL
606
網站之URL已知?
608
否
是
自使用者接收密碼項
610
對密碼加密 612
將加密密碼與URL關聯地保存
614
自記憶體擷取加密密碼
616
偵測到經認證之指紋？
618
否
是
向網站提供破解之密碼
620

【圖 6】


700
自指紋感測器接收表示
第一指紋之第一信號
702
第一信號與同警示條件
相關聯之資料相匹配？
704
是
產生警示 706
否
第一信號與第一所
儲存資料相匹配？
708
否
結束
是
自指紋感測器接收
表示第二指紋之第二信號
710
第二信號與同警示
條件相關聯之資料相匹配？
712
是
否
7B

【圖 7A】


700
7A
第二信號與第二所儲存資料相匹配？
714
否
結束
是
識別第一信號及第二信號之時間順序
716
時間順序與預定義順序相匹配？
718
否
結束
是
產生命令 720

【圖 7B】