公告本

申請日期	88. 11. 23
案號	88120472
類別	H04L 9/32, 9/10

（以上各欄由本局填註）

A4
C4

511362

發明 新型 專利說明書

一、發明 新型 名稱	中文	藉需密鑰式取樣保護生物特質資料之方法與系統
	英文	PROTECTION OF BIOMETRIC DATA VIA KEY-DEPENDENT SAMPLING
二、發明 創作 人	姓名	1. 史帝芬 M. 麥提亞 2. 穆罕默德派瑞韋恩
	國籍	1. 美國　2. 美國
	住、居所	1. 美國維吉尼亞州麥納薩斯細達山脈大道 10298 號 2. 美國北卡羅萊納州蓋瑞雷克荷羅圓環 122 號
三、申請人	姓名（名稱）	美商・萬國商業機器公司
	國籍	美國
	住、居所（事務所）	美國紐約州阿蒙市新果園號
	代表人姓名	傑拉德羅森瑟爾

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）　申請專利，申請日期：　　案號：　　，☑有　□無主張優先權

本案已向美國申請專利；申請日：1999 年 1 月 27 日　案號：09/238,700 號

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（　）

發明領域：

本發明係有關於一種用以識別及/或確認之系統與方法和電腦程式產品，且更明確地是，一種有關於使用生物特質資料以識別及/或確認個人之系統、方法與電腦程式產品。

發明背景

生物特質資訊現在係以作為對個人的一種辨識及/或確認技術而使用。對於熟稔本項之技藝人士而言，生物特質資訊是個人的一或多種行為及/或生理上的特性。生物特質辨識及/或確認使用一個資料處理系統，可藉生物特質特徵之電腦評估作業，而進行自動身分辨識及/或確認。在生物特質確認作業中，係對一已知的個人進行生物特質資訊確認。而在生物特質辨識中，某個人的生物特質資訊會與已知之諸生物特質資訊進行比對，以便識別該個人。

該生物特質辨識/確認系統、方法和電腦程式產品，能測量單一或眾人下列之行為及/或生理學的特性：指紋、手型幾何、虹膜模型、臉部特性、聲音特徵、筆跡動力學、耳垂特點和按鍵動力學。而也可以使用其他的生物特質特徵。生物特質技術的應用則包括生物特質支票兌現機、付款系統，而以生物特質資料來取代個人辨識號碼；使用生物特質資料、生物特質職員時間和出席紀錄，以及用於運輸方面之生物特質乘客控制的存取控

五、發明說明（　）

制系統。許多其他應用亦可採用生物特質資訊來進行辨識及/或確認。請參閱標題為「Biometrics, Is it a Viable Proposition for Identity Authentication and Access Control」Kim，「電腦與安全」，Vol 14，1995，pp.205-214；「A Robust Speaker Verification Biometric」，George et al.，IEEE 29th，1995 年十月進行中的國際 Carnahan 有關安全技術之會議，pp.41 到 46；「On Enabling Secure Applications Through Off-line Biometrics Identification」，Davida et al.，IEEE 電腦社團對安全和隱私所進行的研究，1998，pp. 148-157；以及「Biometric Encryption：Information Privacy in a Networked World」，Brown et al.，EDI 論壇：電子商務日報，v.10， No.3，1997，pp. 37-43。

第 1 圖為一傳統性的生物特質辨識及/或確認系統、方法和電腦程式產品之區塊圖。在第 1 圖內，生物特質辨識及/或確認出現於使用網際網路嵌入檔的「客戶端-伺服器」環境中。對於熟稔本項之技藝人士而言為眾知，伺服器為執行於一電腦及/或一特定目的硬體上之電腦及/或軟體程式，提供特定服務種類予客戶端。而客戶端則是執行於一電腦及/或一特定目的硬體上之電腦及/或軟體程式，用來接觸而且獲取透過通訊網路而由伺服器所傳來的資料。該客戶端和伺服器每個可能包含單一或多個主機，中級及/或個人電腦，及/或執行於一個或多個彼等電腦及/或一特定目的硬體上之一個或多個應用程式。該

五、發明說明（　）

客戶端和伺服器可執行在相同的電腦或不同的電腦上。該網路可為一區域網路，廣域網路，網際網路，一應用程式界面以及任何其他可用來連接一客戶端和一伺服器的通訊機制。當使用網際網路來作為客戶端和伺服器之間的通訊網路時，可採用網頁瀏覽器當作為客戶端，而其網頁伺服器可作為伺服器。

現參考第 1 圖，一客戶端 10 與位於網際網路 14 上的伺服器 12 進行通訊。該客戶端 10 有一瀏覽器 16，而且該伺服器 12 也有一個網頁伺服器 18。當應用生物特質辨識及/或確認於網際網路上的客戶端和伺服器間之電子商務時，可使用客戶端之生物特質嵌入檔 22 和伺服器生物特質文稿檔 24。譬如說，在此可以使用類似像是 Netscape Communicator 或是 Netscape Navigator 的 Netscape 瀏覽器的生物特質嵌入檔。而在伺服器端，來自客戶端的「全球資源地址碼(URL)」可啟動一個文稿檔，而該文稿檔可包括及/或啟動單一或是多個應用程式來執行生物特質功能。該嵌入檔和文稿檔的設計和使用，對於熟稔本項之技藝人士而言既為眾知，故無須在此作更進一步地描述。

仍請參考第 1 圖，該客戶端生物特質嵌入檔 22 內，包括了生物特質資料獲取 32，可在客戶端執行一個生物特質特徵取樣作業，以產生與生物特質特徵有關的樣本。為了要從客戶端 10 處對該伺服器 12 提供安全的樣本傳輸，該加密模組 34 可使用例如像是「資料加密標準

五、發明說明（　）

(DES)」運算法則的傳統加密技術，來對那些樣本進行加密。可使用一簽章模組 36 以獲致附增之安全性，該簽章模組 36 可採用 RSA 公眾密鑰運算法則，或是其他傳統簽章運算法則，來將一簽章加入那些經加密的樣本中。如此，該客戶端生物特質嵌入檔將在第 1 圖中標示為「ENC(SAMPLE)，SIGNED」經加密和簽章之樣本，經由網際網路 14，自使用瀏覽器 16 的客戶端 10 傳輸到使用網頁伺服器 18 的伺服器 12。

在伺服器 12 處，該伺服器生物特質文稿檔 24 內，包括及/或啟動可以確認該簽章之簽章確認模組 46，例如說使用 RSA 公眾密鑰運算法則，以及例如使用 DES 運算法則來對該經加密之樣本進行解密的解密模組 44。然後可將彼等樣本應用於一銘板比較模組 42，其中在此包含有多個銘板 T1-Tn。該生物特質資料確認的銘板比較技術，對於熟稔本項之技藝人士而言為眾知，故無須在此作更進一步地描述。

不幸地，使用加密及/或簽章可能不適合於生物特質應用程式裡。舉例來說，如果該生物特質資料為 1.2K 位元組之指紋資料，並且已經加密於一智慧卡上，且被傳送到一手指-掃描讀取器以進行確認，則該 RSA 簽章可能會耗用較多的電力和時間，而且可能會產生訊號毀損的風險。該 DES 加密也可使用複雜的主要管理技術，以便在客戶端和伺服器兩端建立一共通之私秘性加密密鑰。因此，使用高度安全性的運算法則，例如 DES 和 RSA

五、發明說明（　）

運算法則可能會加重整體的生物特質應用程式成本及/或複雜性。然而隨著生物特質技術的成本逐漸降低，安全性成本可能就變成一個阻礙生物特質技術廣泛應用的主要因素。此外在某些情況下，複雜的高速加密應用與它的相關的高成本，甚至可能是無法提供保証的。因此，極需要一種能夠在傳輸過程中提供彼等生物特質資料安全保障，而不會非適當地增加生物特質應用程式之成本及/或複雜性的系統、方法和電腦程式產品。

發明目的及概述：

因此，本發明之目的即為提供一經改良之生物特質辨識及/或確認系統、方法和電腦程式產品。

本發明之另一目的為提供一種不需要使用加密及/或簽章，而可將生物特質資料從客戶端傳輸到伺服器的生物特質辨識及/或確認系統、方法和電腦程式產品。

依據本發明，彼等和其他所提供之目的，係於藉由在客戶端執行一個生物特質特徵之密鑰-相關取樣作業，而此產生密鑰-相關之生物特質資料樣本。然後再將該密鑰-相關之生物特質資料樣本，由客戶端傳輸到伺服器。

本發明起源於為從將生物特質資料自客戶端傳輸到伺服器之實際作業，通常是在客戶端對其生物特質特徵進行取樣。藉由以密鑰-相關方式而在客戶端進行生物特質特徵取樣，即可將該密鑰-相關生物特質資料樣本從客戶端傳輸到伺服器，而無須額外的加密及/或簽章。

五、發明說明（　）

依照本發明，該密鑰可由伺服器傳輸到客戶端較佳。然後，可應用該密鑰而於客戶端執行生物特質特徵的密鑰-相關取樣作業。該密鑰-相關取樣作業可以一取樣頻率的方式來對生物特質特徵進行取樣，而該取樣頻率為該密鑰的函數。另一方面，該密鑰可用於彼等經取樣的生物特質資料，藉以產生密鑰-相關並為該密鑰之函數的生物特質資料樣本。在一較佳之具體實施例中，該密鑰用來在客戶端上執行生物特質特徵的非線性密鑰-相關取樣作業，例如說藉由該密鑰以決定其取樣頻率，並且也由該密鑰來將該經取樣之生物特質資料應用於一個非線性函數上。該非線性函數可為例如像是雜湊函數的單向函數。如此，即不需要對該生物特質資料，執行進一步的生物特質資料加密及/或簽章之作業。

在伺服器處，該密鑰也被用於至少一個銘板上，藉此獲取密鑰-相關生物特質資料銘板樣本。然後，在伺服器處，對密鑰-相關之生物特質資料，和至少一個密鑰-相關生物特質資料銘板樣本兩者之間進行比較，以憑識別及/或確認其生物特質特徵。

可以未經保全的方式(公開的方式)，將該密鑰從伺服器傳輸到客戶端。最好是在生物特質特徵取樣之前先行傳輸新的密鑰。另一方面，　如果是已加密狀況，則密鑰亦可予以加密。該密鑰可包括一個以上的數值，以用來執行密鑰-相關之生物特質特徵取樣作業。舉例來說，如果該非線性取樣函數為餘弦函數，則該餘弦函數頻率

五、發明說明（　）

和相位可傳輸作為該密鑰，以統理該施用於經取樣之生物特質資料的取樣速率和函數。另一方面，如果客戶端和伺服器兩者都分享一個私密數值，則該密鑰可為一從伺服器公開傳輸到客戶端的亂數。然後，該亂數可與該私密數值組合應用，以執行該密鑰-相關取樣作業。

因此，生物特質資料可以未加保全的方式，被從一客戶端傳輸到一伺服器，而不需要複雜的加密及/或簽章。如此，即可以有效率的方式來提供未加保全的電子商務。應瞭解本發明之形式可為系統、方法及/或電腦程式產品。

圖式簡單說明：

第 1 圖為以傳統網際網路為基礎之客戶端伺服器的生物特質系統、方法和電腦程式產品的區塊圖。

第 2 圖為符合本發明，而以網際網路為基礎之客戶端伺服器生物特質系統、方法和電腦程式產品的區塊圖。

第 3 圖生物特質資料傳輸之流程圖。

第 4 圖為一說明符合本發明的生物特質資料處理流程圖。

第 5 圖為說明傳統性生物特質特徵之圖形。

第 6 圖及第 7 圖為說明符合本發明的密鑰-相關生物特質資料之圖形。

五、發明說明（　）

圖號對照說明：

10	客戶端	12	伺服器
14	網際網路	16	瀏覽器
18	網頁伺服器	22	客戶端生物特質嵌入檔
24	伺服器端生物特質文稿檔		
32	生物特質資料獲取	34	加密模組
36	簽章模組	42	銘板比較模組
44	解密模組	46	簽章確認模組
110	客戶端	112	伺服器
114	網際網路	116	網頁瀏覽器
118	網頁伺服器		
122	客戶端生物特質嵌入檔		
124	伺服器之生物特質文稿檔		
132	生物特質資料獲取	142	銘板比較模組
148	密鑰-相關銘板區塊		

發明詳細說明：

後文將對於本發明作進一步說明並惠請參酌隨附圖示，其中係以圖型表示本發明之較佳具體實施例。然而，本發明可以許多不同型式來具體實作，故而不應將其解釋為限制於文中所述之彼等具體實施例；相反地，提供該等具體實施例，係為徹底及完整說明本揭示，並且可對彼等熟稔本項技藝之人士完全傳達本發明之範圍。全文內相同之數字係指相同之元件。

五、發明說明（　）

正如熟稔本項技藝之人士所知，本發明可能被具體製作為系統(裝置)、方法及/或電腦程式產品。因此，本發明可為完全是硬體之具體實施例之形式，完全是軟體之具體實施例或軟硬體方面所組合之具體實施例。此外，本發明可為電腦-可讀取儲存媒體上的電腦程式產品形式，其中該儲存媒體具有實作於該媒體中的電腦-可讀取程式碼裝置。在此，可選用任何包括硬碟、CD-ROM、光學儲存裝置或是磁性儲存裝置的適當電腦可讀取媒體。

現參考第 2 圖，茲對該符合本發明並可安全地傳輸生物特質資料之客戶端-伺服器系統、方法和電腦程式產品進行說明。如同前述，客戶端 110 和伺服器 112 可為一主機、中級及/或個人電腦，其中並且/或者單一或多個應用程式執行於上述這些電腦及/或特定目的硬體之上。客戶端 110 和伺服器 112 可在相同的電腦上執行。然而，為便於說明，第 2 圖內係以範例來敘述使用網際網路 114，將生物特質資料從客戶端 110 傳輸到伺服器 112 的電子商務系統、方法和電腦程式產品，其中該客戶端 110 使用網頁瀏覽器 116，而該伺服器 112 使用網頁伺服器 118。

續參考第 2 圖，該客戶端 110 中包括一具有生物特質資料獲取 132 的客戶端生物特質嵌入檔 122，而該嵌入檔可在客戶端執行一個生物特質特徵的密鑰-相關取樣作業，藉此產生密鑰-相關生物特質之資料樣本。可將那

五、發明說明（　）

些密鑰-相關樣本，透過網際網路 114 而傳送給伺服器 112，而不需要使用例如像是 DES 運算法則的額外加密作業，同時也不需要使用例如 RSA 運算法則的公眾密鑰運算法則之簽章作業。

在伺服器 112，伺服器生物特質之文稿檔 124 可由網頁伺服器 118 獲得該等密鑰-相關樣本。而且至少會執行一個銘板 T1-Tn 的密鑰-相關取樣作業，以分別在區塊 140 和 148 處，取得至少一個密鑰-相關之銘板 T1(k)-Tn(k)。該銘板比較模組 142 會將至少一個密鑰-相關銘板 T1(k)-Tn(k)的與自網頁伺服器 118 處所獲得之密鑰-相關樣本進行比較，以確認及/或識別該生物特質資料。該伺服器生物特質文稿檔可包括及/或啟動一個或多個應用程式以取得銘板(區塊 140 處)，產生該密鑰-相關銘板(區塊 148 處)，而且執行一比較作業(區塊 142 處)。另一方面，該應用程式可介接於應用程式界面(API)，提供硬體及/或軟體性加密服務。該文稿檔之設計和操作對於熟稔本項技藝人士而言為眾知，故無須在此作更進一步地描述。

現參考第 3 圖，其中將說明該符合本發明之生物特質資料傳輸。如區塊 310 所示，首先從伺服器 112 處傳輸一密鑰到客戶端 110。如同後文詳述，該密鑰可為一單一亂數、多個亂數或是其他的數值組合，可用來設定取樣頻率及/或非線性函數內其他的取樣參數，該函數係用以於客戶端處執行生物特質特徵的非線性密鑰-相關取樣作業。因此，在區塊 320 處，生物特質特徵是按照密

五、發明說明（　）

鑰-相關樣本頻率而加以取樣。舉例來說，某個在第 5 圖中顯示為時間及/或空間的函數之生物特質特徵，在第 6 圖裡係以一取樣頻率 T 而被取樣，此為該密鑰的函數。所以，可將該密鑰 T 從伺服器 112 處傳輸到客戶端 110 處，藉此來提供對該生物特質特徵進行取樣時所用的取樣頻率 T。該密鑰-相關生物特質資料樣本的真值可由第 6 圖內的細點顯示之。

現參考第 3 圖中的區塊 330，該密鑰它本身也可應用於該經取樣之生物特質特徵，以使得該等所獲得之真值，與密鑰-相關生物特質資料的真值兩者之間，其差值為一非線性函數。因此，如第 7 圖所示，該密鑰適用於第 6 圖內的經取樣之生物特質資料，藉以產生在第 7 圖裡以細點顯示之密鑰-相關生物特質資料樣本。該密鑰-依賴生物特質資料最好是與第 6 圖的真實生物特質資料樣本之間具有非線性的相關性。彼等亦可為生物特質資料樣本的單向非線性函數，例如一個雜湊函數。最後，如第 3 圖的區塊 340 所示，將該密鑰-相關樣本傳送到伺服器 112 處。

在伺服器 112 處，該生物特質資料處理如第 4 圖所示進行。在區塊 410 處，對一個或更多的銘板 T1-Tn 以密鑰-相關樣本頻率進行取樣，並且在區塊 420 處，將該密鑰應用於樣本銘板，藉此產生如第 2 圖的密鑰-相關銘板 T1(k)-Tn(k)。最後，在區塊 430 處，該密鑰-相關銘板 148 會與由網頁伺服器 118 所獲得密鑰-相關樣本進行比

五、發明說明（　）

較，藉以確認及/或識別那些生物特質資料。

再一次參考到第 2 至第 7 圖以討論一範例，其中如第 5 圖的生物特質特徵，為一連續性的語音輸入訊號 $\nu(T)$，該 T 表示時間。該等生物特質資料獲取模組 132 內的感測裝置，將語音輸入訊號轉換成為每隔 T 秒最靠近該訊號振幅而以量化方式表示之振幅值的二進位碼，其中該 T 為取樣時段。如此，取樣頻率即為 F = 1/T 赫茲。由於該取樣作業係按照取樣頻率的非線性函數，故該取樣頻率可用來作為該項作業的密鑰。例如，可如下列各式，藉一餘弦函數而獲得生物特質特徵的密鑰-相關樣本：

$$c(n) = \nu(n.T) \times \cos[B \times (n.F + F_0)] \quad \text{對於} \quad n \$ 0$$

其中

c(n) 為在點 n 上的密鑰-相關樣本，

$\nu(n.T)$ 在點 n 上被取樣的訊號，和

F_0 為相位位移。

因此，密鑰-相關樣本 c(n)係以非線性的方式，由該密鑰頻率 F 和 F_0 所決定。經由網際網路 114，將該密鑰-相關樣本傳輸給使用著瀏覽器 116 的客戶端 110，而由伺服器 112 處的網頁伺服器 118 所接收。

為進行辨識及/或確認，在伺服器 112 處，利用該密鑰頻率 F 和 F_0，由預先儲存的銘板 T1-TB 至少其中一個，藉前文所述的銘板資料之密鑰-相關取樣作業方式，來產生至少一個密鑰-相關銘板 T1(k)-Tn(k)。至於確認作業，

五、發明說明（　）

可對該密鑰-相關銘板與密鑰-相關樣本兩者間進行比較，以決定該兩者是否來自於相同的使用者。辨識作業可以與其類似的方式執行，但是在這情況之下，該密鑰或將用以由彼等經預先儲存的銘板來產生多個密鑰-相關銘板。然後，比較該密鑰-相關樣本與該密鑰-相關銘板，俾決定使用者的身份。

對於熟稔本項技藝之人士，應了解到在執行生物特質取樣操作之前，必須先行將該密鑰分別地安裝或設定於客戶端 110 和伺服器系統 112。若因其他的理由，該密碼機制已出現在客戶端和伺服器上，則該伺服器即可使用公眾-密鑰或對稱-密鑰的密碼法則，來將該密鑰(例如 F 和 F_0 的密鑰)傳送給伺服器，並藉此對密鑰提供更高的安全性。另一方面，該密鑰可以公開方式從伺服器 112 傳輸到客戶端 110。只要該密鑰的空間足夠大，而讓攻擊者無法攔截充份的傳輸生物特質資料與密鑰而變造出新的被攔截密鑰之生物特質樣本的話，那麼公開的密鑰傳輸仍然是可以保障生物特質資料傳輸的安全性。如果資訊內容中有極多的生物特質樣本，而且也包含了很多的資料，那麼密鑰-相關取樣即無須干涉該使用者辨識或使用者確認功能的堅韌性，其中可對該密鑰-相關樣本以及該密鑰-相關銘板加以比較或分析，以決定他們是否是來自於相同使用者的生物特質資料。如此，當資訊內容和生物特質樣本的數量持續增加時，以公開方式將密鑰從伺服器 112 傳輸到客戶端 110 可能會比較具有實用性。

五、發明說明（　）

在其它的替代方案中，該密鑰不以公開方式傳輸。相反地，客戶端 110 和伺服器 112 共有一秘密數值 S。該伺服器 112 將一亂數 R 以公開方式送往客戶端 110。該亂數可與該秘密數值組合使用，以執行密鑰-相關取樣。如同上述的語音取樣範例，所導得的密鑰可為密鑰頻率 F 和 F_0。這是可以做到的，例如藉由一個雜湊函數，例如下列在經連結的 S 和 R 值上的傳統 SHA-1 式：

Key = SHA-1 (S,R)

應了解在該密鑰分配方法中，對於該共通之秘密數值 S 會先在每個裝置內設定初值。然而，因為該等密鑰並非以公開方式傳輸，因此這技術尚有諸項優點，故某攻擊者不可能知道從 S 和 R 值所產生出來的密鑰，只要該 R 值足夠大以致於不太可能重複。因此，攻擊者通常不會知道將他自己的密鑰-相關生物特質樣本，替換為哪個密鑰-相關生物特質樣本，才能夠模仿為另外的一個使用者。而且，該密鑰導出運算法則可能很簡單和直接。因此，當客戶端和伺服器需要實作該密鑰導出運算法則時，即不需要實作一加密運算法則。

辨識/確認作業上可假定每個密鑰-相關生物特質樣本，以及其關連的密鑰-相關銘板係唯一地成對，並且對第一個密鑰所獲得的密鑰-相關生物特質樣本，將無法由第二個不同密鑰的密鑰-相關銘板而被獲致核可。因此，密鑰-相關樣本的構成方式，應該是要讓那些所獲取到的生物特質樣本，對於每個密鑰而言均為不同，換言之，

五、發明說明（　）

足夠地不同，而可在辨識/確認程序裡達成上述細節。

在上述語音取樣例子中，如果是以由二個至少在一個樣本點上為相異的密鑰-相關樣本集合中的方式來選擇該等密鑰的話，則為第一個密鑰所獲得的密鑰-相關生物特質樣本，通常不會讓不同的第二密鑰之密鑰-相關銘板被核可。這是因為對於至少一個樣本點 i，該 c'(i)≠c"(i)，也就是說下列各項不等式可成立：

$$c'(i) = v'(i.T') \times \cos[B\times (i.F' + F_0')] \neq c''(i) = v''(i.T'') \times \cos[B\times (i.F'' + F_0'')]$$

如該密鑰頻率範圍足夠大，則以隨意方式選取密鑰頻率，即可滿足上述的需求，而甚有可能獲得針對各個密鑰的不同生物特質樣本。

本發明所適用的另外一個生物特質系統，是由位於 Wellesley，MA 的 Miros 公司所銷售的電腦程式產品，稱為「TrueFace」，可提供網際網路網站接取保全服務。請參閱 www.miros.com。該「TrueFace」產品係採用微軟公司 ActiveX 技術來下載面部捕捉軟體，以提供給上網之電腦使用者的瀏覽器。該 ActiveX 元件將那些被抓取到的資料，交返到該 TrueFace 伺服器元件可藉由已登記的影像而來對該上網者進行確認的網站位置處。伺服器軟體執行於視窗 NT 上，而客戶端則是使用微軟公司的網際網路 Explorer 或是 Netscape 航海家的嵌入檔。對於該生物特質系統可能的攻擊方式，會是在傳輸過程中(由伺服器到客戶端)某攻擊者首先攔截到生物特質樣本，然後

五、發明說明（　）

再藉由執行一線上攻擊，在其中會將該攻擊者的生物特質資料，被那些所攔截到的生物特質資料加以替換，因而模仿成其他的使用者。

不需對所傳輸的生物特質資料加密，該等生物特質資料可透過使用根據本發明之密鑰-相關取樣方法而受到保護。在此情況下，該伺服器可產生一個密鑰而且將其傳送到瀏覽器，舉例來說，連同從伺服器下載的面部捕捉軟體一起送出。接著，該面部捕捉軟體將使用該密鑰來執行一密鑰-相關取樣作業，以取得一相對應的密鑰-相關生物特質面部樣本，再以公開方式將該樣本會被送至伺服器。該伺服器會使用該密鑰來過濾出一經儲存的生物特質銘板，以產生密鑰-相關生物特質銘板樣本，再將所產生的樣本與從客戶端所收到的密鑰-相關生物特質面部樣本進行或分析，以決定這兩份生物特質資料是否來自於相同的使用者。如果該密鑰和密鑰-相關的數字生物特質面部樣本足夠大，那麼該攻擊者即無法偽造出某個被看到(或是攔截到)密鑰的密鑰-相關生物特質面部資料。

在另外的一個例子中，一智慧卡製造業者 On Track Innovation 公司(OTI)已將一種指紋生物測定技術，整合到該公司使用 Identix's「Fingerscan」技術的「Eyecom」無接觸型智慧卡之上。請參閱該網址 www.oti.co.il.。在卡片和該掃描終端機之間的資料交換，只會以短暫無接觸的電力窗口「動態」方式來進行交換該生物特質銘板。

五、發明說明（　）

使用 DES 或是 RSA 公眾密鑰加密技術來對 1.2K 位元組銘板加密，以便將其無線傳輸給 Fingerscan 讀取機進行確認作業。該確認程序是私屬性的並且為區域性的，並沒有使用到任何網路。

本發明可以依下列各項加以應用：接著 Fingerscan 讀取機可產生以公開方式傳送到智慧卡的密鑰。回應於此，該智慧卡可使用該密鑰來過濾出經儲存的生物特質銘板，以產生出具有唯一性的密鑰-相關生物特質銘板，然後將其傳輸給 Fingerscan 讀取機。該 Fingerscan 讀取機接著會藉該密鑰，來執行一應用到指紋掃描技術之密鑰-相關取樣作業，俾取得對應的密鑰-相關生物特質樣本，然後再將該取得的樣本與從智慧卡所收到的密鑰-相關生物特質銘板進行比較及分析。

某闖入者即使是攔截到一個，或者是許多個，密鑰和其密鑰-相關生物特質銘板，也不會有足夠的資訊來偽造生物特質資料，因為指紋掃描技術所選擇的密鑰，並不必然會與被闖入者所攔截到的任何密鑰其中之一相符。因此，闖入者就沒有如欲偽造那些生物特質資料時所需要的生物特質資訊。應了解到該安全性係與足夠大的密鑰-空間有關，以便讓闖入者無法收集充份的生物特質銘板，來偽造由指紋掃描技術所任意選擇之密鑰的生物特質資料。

因此，可藉由生物特質特徵的密鑰-相關取樣，來提供從客戶端到伺服器之生物特質資料安全性傳輸，而無

五、發明說明（　）

須予以加密及/或簽章。按此即可提供經改良的生物特質測知系統、方法和電腦程式產品。

在附圖中詳細地敘述本發明各種不同的外觀，其中包括流程圖說明。應了解到圖式中的個別區塊，以及圖式中區塊之組合，可由電腦程式指令加以實作。並且可將該等電腦程式指令提供至一處理器或其他的可程式化資料處理裝置以製作一機器，使得那些執行於處理器或是其他的可程式化資料處理裝置上的指令，可產生實作該等在諸區塊中所述之功能的裝置。也可將這些電腦程式指令儲存於一電腦可讀取記憶體內，以特定方式來指示該處理器或其他的可程式化資料處理裝置進行作業，而讓那些儲存於電腦可讀取記憶體內指令，可產生一種製造物件，其中包含有指令裝置以實作該等在諸區塊中所述之功能。因此，圖中各個區塊可支援諸執行該等所述功能的裝置之組合、諸執行該等所述功能的步驟之組合，以及諸執行該等所述功能的程式指令裝置。亦應了解圖中之個別區塊，和彼等流程圖裡的諸區塊之組合，可以被執行特定目的之硬體為基礎的電腦系統而予以實作，其中該系統可執行所述之功能或步驟，或者是由特定目的硬體和電腦指令之組合而予以實作。

在圖示和規格中，已揭示本發明一般較佳之具體實施例，並且雖然使用特定術語，然本發明範圍係列述於下列各項申請專利範圍內，不過僅以通用性和描述性觀點而述，並不具限制性目的。

A5
B5

四、中文發明摘要（發明之名稱：　　）

藉需密鑰式取樣保護生物特質資料之方法與系統

於客戶端執行一種生物特質特徵的密鑰-相關取樣，藉此產生密鑰-相關生物特質資料樣本。然後將該密鑰-相關生物特質資料樣本，從客戶端傳輸到伺服器。藉由以此種密鑰-相關方式來在客戶端進行生物特質特徵取樣，即可將該密鑰-相關生物特質資料樣本由從客戶端傳輸到伺服器，而無須額外的加密及/或簽章作業。該密鑰最好是從伺服器傳輸到客戶端。然後在客戶端利用該密鑰來執行密鑰-相關生物特質特徵之取樣作業。該密鑰-相關取樣作業，可以一個取樣頻率來對該生物特質特徵進行取樣，其中該取樣頻率為密鑰的函數。另外地，該密鑰可

英文發明摘要（發明之名稱：　**PROTECTION OF BIOMETRIC DATA VIA KEY-DEPENDENT SAMPLING**　）

Key-dependent sampling of a biometric characteristic is performed at a client, to thereby generate key-dependent biometric data samples. The key-dependent biometric data samples are then transmitted from the client to a server. By sampling the biometric characteristic at the client in a key-dependent manner, the key- dependent biometric data samples may be transmitted from the client to the server without the need for additional encryption and/or a signature. A key is preferably transmitted from the server to the client. The key is then used to perform the key- dependent sampling of the biometric characteristic at the client. The key-dependent sampling may be performed by sampling the biometric characteristic at a sampling frequency that is a function of the key.

A5
B5

四、中文發明摘要（發明之名稱：　　）

適用於彼等經取樣之生物特質資料，藉以產生密鑰-相關生物特質資料樣本，而該樣本為密鑰的函數。該密鑰較適宜用來在客戶端執行非線性密鑰-相關生物特質特徵取樣，例如使用該密鑰來決定該取樣頻率並且也對那些經取樣的生物特質資料，藉該密鑰而應用於一非線性函數。如此，即不需要執行彼等生物特質資料進一步加密及/或生物特質資料簽章等作業。

英文發明摘要（發明之名稱：　　）

Alternatively, the key can be applied to the sampled biometric data, to thereby generate the key-dependent biometric data samples that are a function of the key. The key is preferably used to perform nonlinear key- dependent sampling of the biometric characteristic at the client, for example by using the key to determine the sampling frequency and also using the key to apply a nonlinear function to the sampled biometric data. Further encryption of the biometric data and/or the use of a signature with the biometric data need not be performed.

A8
B8
C8
D8

六、申請專利範圍

1. 一種為將生物特質資料從一個客戶端安全地傳輸到一伺服器之方法，其中包含下列步驟：

在客戶端執行一生物特質特徵的密鑰-相關取樣，藉以產生密鑰-相關生物特質資料樣本；和

將密鑰-相關生物特質資料樣本從客戶端傳輸到伺服器。

2. 如申請專利範圍第1項所述之方法，其中上述之執行步驟是以將密鑰從伺服器傳輸到客戶端來進行，並且該執行步驟中包含有使用該密鑰來在客戶端執行生物特質特徵之密鑰-相關取樣的步驟。

3. 如申請專利範圍第1項所述之方法，其中上述之執行步驟包含下列步驟：

以一取樣頻率來對生物特質特徵進行取樣，其中該取樣頻率為密鑰一個函數。

4. 如申請專利範圍第1項所述之方法，其中上述之執行步驟包含下列步驟：

對生物特質特徵進行取樣，以獲得取樣生物特質資料；和

對經取樣的生物特質資料應用該密鑰，藉此產生密鑰-相關生物特質資料樣本。

六、申請專利範圍

5. 如申請專利範圍第1項所述之方法，其中上述之執行步驟包含下列步驟：

以一取樣頻率來對生物特質特徵取樣，該取樣頻率是密鑰的函數，藉此獲得經取樣之生物特質資料；和

將該密鑰應用於該經取樣之生物特質資料，藉此產生密鑰-相關生物特質資料樣本。

6. 如申請專利範圍第1項所述之方法，其中上述之執行步驟包含下列步驟：

在客戶端執行生物特質特徵的非線性密鑰-相關取樣，藉此產生密鑰-相關生物特質資料樣本。

7. 如申請專利範圍第1項所述之方法，其中上述之傳輸步驟係包括下列步驟：

將該密鑰-相關生物特質資料樣本，與至少一個密鑰-相關生物特質資料銘板在伺服器進行比較。

8. 如申請專利範圍第2項所述之方法，其中上述之傳輸步驟係包括下列步驟：

從伺服器傳輸一個亂數到客戶端；和

在客戶端將亂數和一私密數值加以組合；和

其中該執行步驟，包含有密鑰-相關的執行步驟

利用該亂數以及私密數值的組合而加以取樣。

六、申請專利範圍

9. 如申請專利範圍第8項所述之方法，其中在進行傳輸該亂數之步驟前，先將該私密數值從伺服器傳輸到客戶端。

10. 如申請專利範圍第1項所述之方法，其中上述之傳輸步驟包括在網際網路上將密鑰-相關生物特質資料樣本從客戶端傳輸到伺服器之步驟。

11. 一種在伺服器處理來自於客戶端的生物特質資料之方法，包含下列步驟：

在伺服器處執行至少一個生物特質特徵的銘板密鑰-相關之取樣作業，藉以產生密鑰-相關生物特質銘板資料樣本；和

將密鑰-相關生物特質銘板資料樣本與來自客戶端的那些生物特質資料進行比較。

12. 如申請專利範圍第11項所述之方法，其中上述之執行步驟包含了下列步驟：

以一取樣頻率來對生物特質特徵銘板取樣，該取樣頻率是密鑰的函數。

13. 如申請專利範圍第11項所述之方法，其中上述之執行步驟包含了下列步驟：

對該至少一個生物特質特徵銘板進行取樣，以取得取

六、申請專利範圍

樣生物特質銘板資料；和

應用該密鑰於那些經取樣之生物特質銘板資料，藉以產生密鑰-相關生物特質銘板資料樣本。

14. 如申請專利範圍第11項所述之方法，其中上述之執行步驟包含下列步驟：

以一取樣頻率來對生物特質特徵銘板取樣，該取樣頻率是密鑰的函數，以獲得取樣生物特質銘板資料；和

應用該密鑰於那些經取樣之生物特質銘板資料，藉以產生密鑰-相關生物特質銘板資料樣本。

15. 如申請專利範圍第11項所述之方法，其中上述之執行步驟包含下列步驟：

在伺服器處對至少一個生物特質特徵銘板執行非線性密鑰-相關取樣，藉以產生密鑰-相關生物特質銘板資料樣本。

16. 一個用以安全地傳輸生物特質資料之客戶端系統，其中包含：

用來進行生物特質特徵之密鑰-相關取樣，藉以產生密鑰-相關生物特質資料樣本的諸項裝置；和

用來將密鑰-相關生物特質資料樣本傳輸至一伺服器的諸項裝置。

六、申請專利範圍

17. 如申請專利範圍第16項所述之系統，其中更包含用以自伺服器處接收密鑰的諸項裝置，以及其中該執行裝置係包括有使用該密鑰來進行生物特質特徵的密鑰-相關取樣之諸項裝置。

18. 如申請專利範圍第16項所述之系統，其中上述之執行裝置包含：

以一取樣頻率來對生物特質特徵取樣，該取樣頻率是密鑰的函數。

19. 如申請專利範圍第16項所述之系統，其中上述之執行裝置包含：

對生物特質特徵進行取樣，以獲得取樣生物特質資料之裝置；和

應用該密鑰於那些經取樣之生物特質資料，藉以產生密鑰-相關生物特質資料樣本之裝置。

20. 如申請專利範圍第16項所述之系統，其中上述之執行裝置包含：

以一取樣頻率來對生物特質特徵取樣，而該取樣頻率是密鑰的函數，以獲得取樣生物特質資料之裝置；和

應用該密鑰於那些經取樣之生物特質資料，藉以產生密鑰-相關生物特質資料樣本之裝置。

六、申請專利範圍

21. 如申請專利範圍第16項所述之系統，其中上述之執行裝置包含：

執行生物特質特徵的非線性密鑰-相關取樣，藉此產生密鑰-相關生物特質資料樣本之裝置。

22. 如申請專利範圍第16項所述之系統，其中上述之執行裝置包含一執行生物特質特徵銘板的密鑰-相關取樣之裝置，藉此產生密鑰-相關生物特質資料銘板樣本。

23. 如申請專利範圍第16項所述之系統，其中上述之執行裝置包含：

一接收來自伺服器的亂數之裝置；

一在客戶端將該亂數和一私密數值加以組合之裝置；和

一使用該經組合之亂數與該私密數值，來進行密鑰-相關取樣之裝置。

24. 如申請專利範圍第23項所述之系統，其中上述之執行裝置更包含用以接收來自伺服器的私密數值之裝置。

25. 如申請專利範圍第16項所述之系統，其中上述之傳輸裝置包含一網頁瀏覽器，以透過網際網路將密鑰-相關生物特質資料樣本傳輸至伺服器。

26. 一種用以處理生物特質資料的伺服器系統，其中包

六、申請專利範圍

含：

用以對至少一個生物特質特徵銘板的密鑰-相關進行取樣，藉此產生密鑰-相關生物特質銘板資料樣本之裝置；和

將該密鑰-相關生物特質銘板資料樣本與來自客戶端的生物特質資料兩者進行比較之裝置。

27. 如申請專利範圍第26項所述之系統，其中上述之執行裝置包含：

以一取樣頻率來對生物特質特徵銘板取樣之裝置，該取樣頻率是密鑰的函數。

28. 如申請專利範圍第26項所述之系統，其中上述之執行裝置包含：

對該至少一個生物特質特徵銘板進行取樣，以取得取樣生物特質銘板資料之裝置；和

應用該密鑰於那些經取樣之生物特質銘板資料，藉以產生密鑰-相關生物特質銘板資料樣本之裝置。

29. 如申請專利範圍第26項所述之系統，其中上述之執行裝置包含：

以一取樣頻率來對至少一個生物特質特徵銘板取樣，該取樣頻率是密鑰的函數，以獲得經取樣生物特質銘板資料之裝置；和

六、申請專利範圍

應用該密鑰於那些經取樣之生物特質銘板資料，藉以產生密鑰-相關生物特質銘板資料樣本之裝置。

30. 如申請專利範圍第26項所述之系統，其中上述之執行裝置包含：

對至少一個生物特質特徵銘板進行非線性密鑰-相關取樣，藉以產生密鑰-相關生物特質銘板資料樣本之裝置。

31. 一種用以安全地傳輸生物特質資料的電腦程式產品，該電腦程式產品包含一電腦-可讀取的儲存媒體，其中具有實作於媒體內的電腦-可讀取程式碼裝置，該電腦-可讀取程式碼裝置包含：

用以進行生物特質特徵的密鑰-相關取樣作業，藉此產生密鑰-相關生物特質資料樣本的電腦-可讀取程式碼之裝置；和

用以傳輸該密鑰-相關生物特質資料樣本的電腦-可讀取程式碼之裝置。

32. 如申請專利範圍第31項所述之電腦程式產品，其中更包含用以接收密鑰的電腦-可讀取程式碼裝置，並且其中該執行裝置包括使用該密鑰來執行生物特質特徵的密鑰-相關取樣作業。

六、申請專利範圍

33. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

以一取樣頻率來對生物特質特徵取樣的電腦-可讀取程式碼裝置，該取樣頻率是密鑰的函數。

34. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

用來對生物特質特徵取樣，以獲得經取樣之生物特質資料的電腦-可讀取程式碼裝置；和

將該密鑰應用於那些經取樣生物特質資料，藉以產生密鑰-相關生物特質資料樣本的電腦-可讀取程式碼裝置。

35. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

以取樣頻率來對生物特質特徵進行取樣，而其中該取樣頻率是密鑰的函數，藉以獲得經取樣之生物特質資料的電腦-可讀取程式碼裝置；和

應用該密鑰於該經取樣之生物特質資料，藉此產生密鑰-相關生物特質資料樣本的電腦-可讀取程式碼裝置。

36. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

執行生物特質特徵的非線性密鑰-相關取樣，藉此產

六、申請專利範圍

生密鑰-相關生物特質資料樣本的電腦-可讀取程式碼裝置。

37. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置，包含電腦-可讀取程式碼裝置用以進行生物特質特徵銘板的密鑰-相關取樣，藉此產生密鑰-相關生物特質資料銘板樣本。

38. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：
一用以接收亂數之電腦-可讀取程式碼裝置；
為組合該亂數和一私密數碼之電腦-可讀取程式碼裝置；
和
使用經組合的亂數和私密數碼，而執行密鑰-相關取樣之電腦-可讀取程式碼裝置。

39. 如申請專利範圍第38項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置，更包含用以接收該私密數碼的電腦-可讀取程式碼裝置。

40. 如申請專利範圍第31項所述之電腦程式產品，其中上述之電腦-可讀取程式碼傳輸裝置包含一個網頁瀏覽器，可經由網際網路而傳輸該密鑰-相關生物特質資料樣本。

六、申請專利範圍

41. 一種用以處理生物特質資料的電腦程式產品，該電腦程式產品包含了電腦-可讀取的儲存媒體，其中具有實作於該媒體上的電腦-可讀取程式碼裝置，該電腦-可讀取程式碼裝置包含：

對至少一個生物特質特徵銘板進行密鑰-相關取樣，藉此產生密鑰-相關生物特質銘板資料樣本的電腦-可讀取程式碼裝置；和

將該密鑰-相關生物特質銘板資料樣本與生物特質資料兩者進行比較的電腦-可讀取程式碼裝置。

42. 如申請專利範圍第41項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

以一取樣頻率來對該生物特質特徵銘板進行取樣的電腦-可讀取程式碼裝置，其中該取樣頻率為該密鑰的函數。

43. 如申請專利範圍第41項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

對至少一個生物特質特徵銘板取樣，以獲得經取樣之生物特質銘板資料的電腦-可讀取程式碼裝置；和

應用該密鑰於彼等經取樣之生物特質銘板資料，藉此產生密鑰-相關生物特質銘板資料樣本的電腦-可讀取程式碼裝置。

六、申請專利範圍

44. 如申請專利範圍第41項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

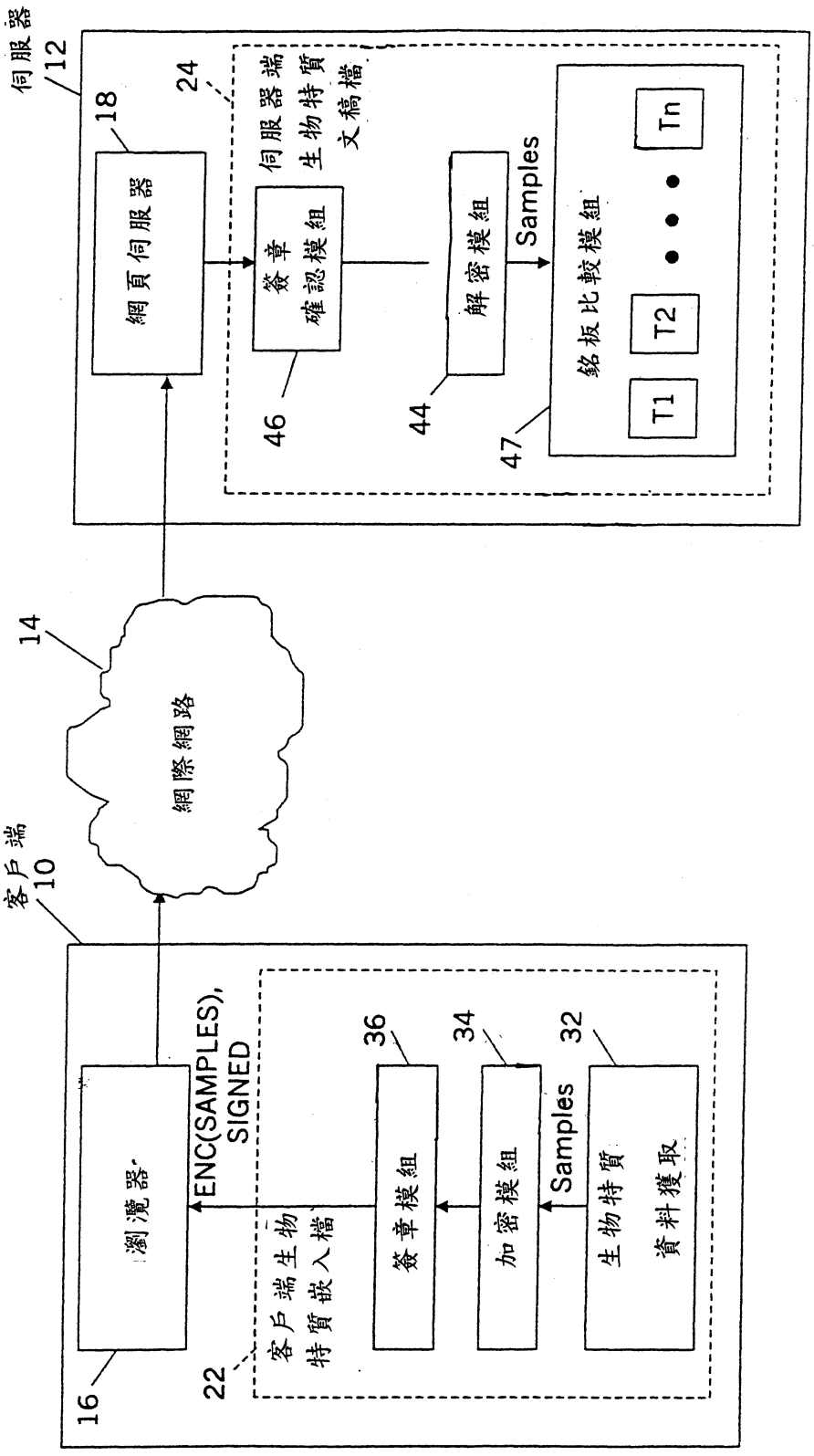
以一取樣頻率來對至少一個該生物特質特徵銘板取樣，其中該取樣頻率為該密鑰的函數，以獲得取樣生物特質銘板資料的電腦-可讀取程式碼裝置；和

應用該密鑰於那些經取樣的生物特質銘板資料，藉此產生密鑰-相關生物特質銘板資料樣本的電腦-可讀取程式碼裝置。

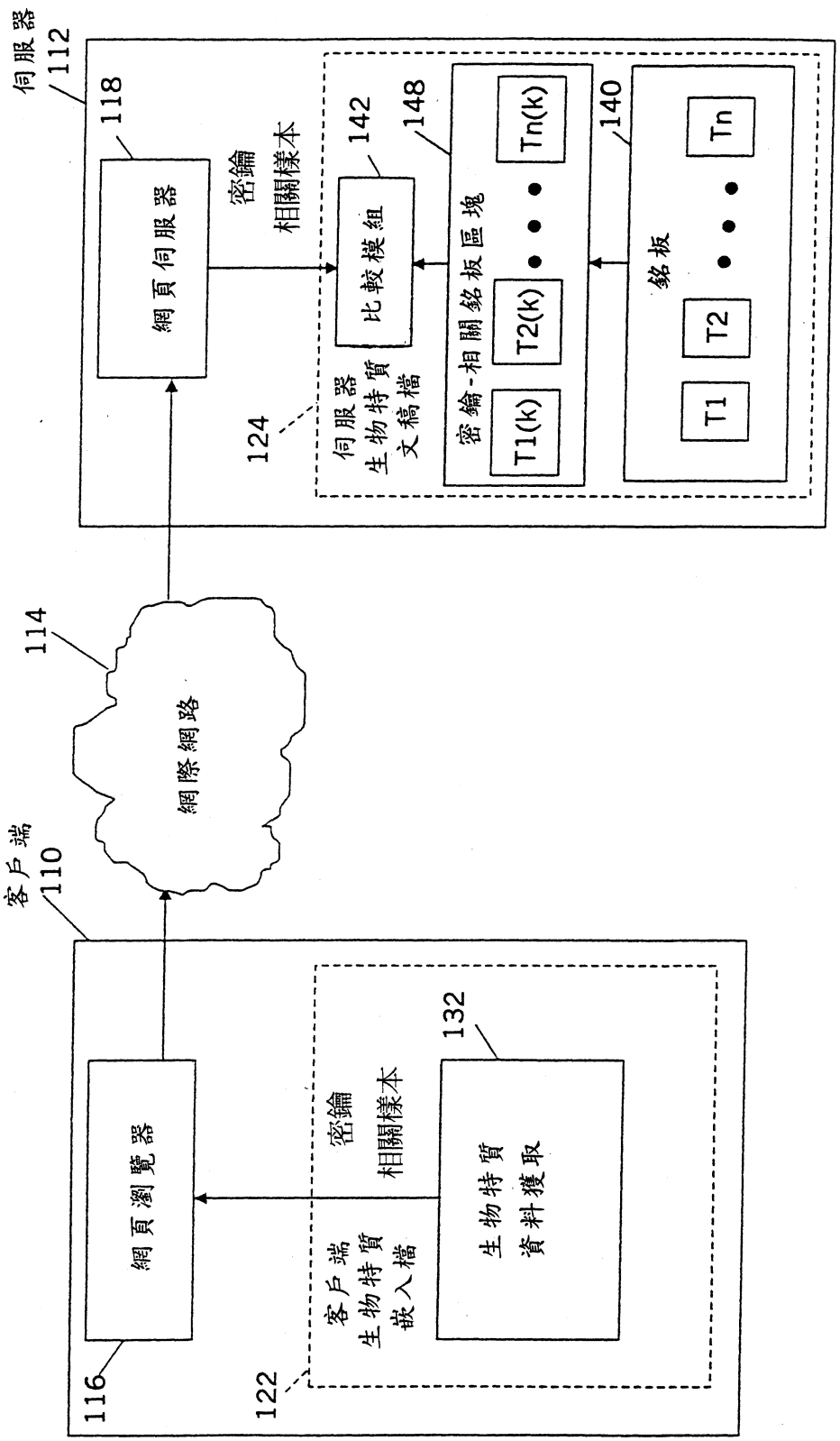
45. 如申請專利範圍第41項所述之電腦程式產品，其中上述之電腦-可讀取程式碼執行裝置包含：

對至少一個生物特質特徵銘板來執行非線性密鑰-相關取樣，藉此產生密鑰-相關生物特質銘板資料樣本的電腦-可讀取程式碼裝置。

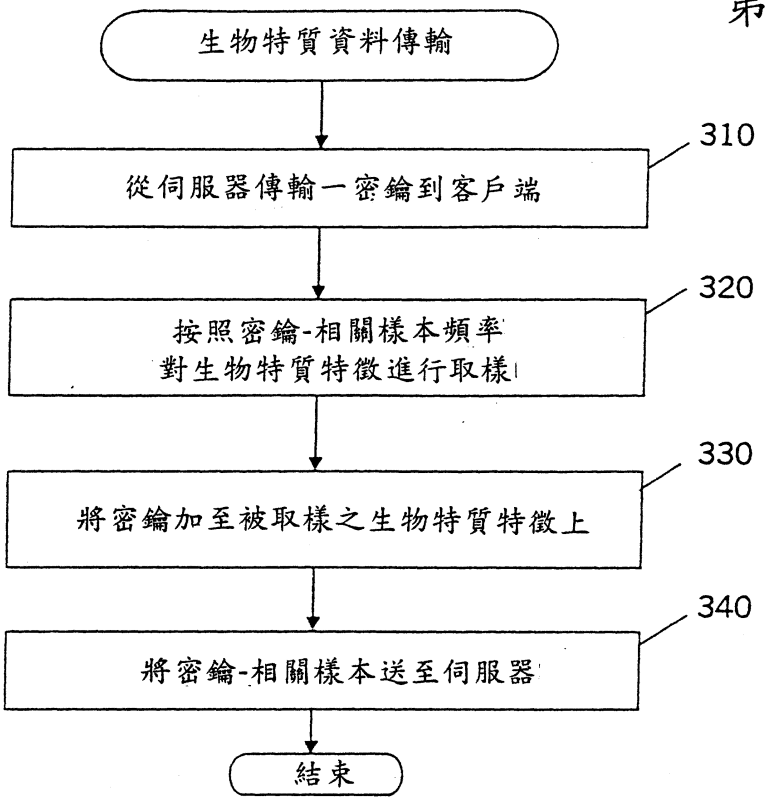
第 1 圖


伺服器
12
網頁伺服器
18
24
伺服器端
生物特質
文稿檔
簽章
確認模組
解密模組
Samples
銘板比較模組
T1
T2
Tn
46
44
47
網際網路
14
客戶端
10
瀏覽器
16
ENC(SAMPLES),
SIGNED
客戶端生物
特質嵌入檔
22
簽章模組
36
加密模組
34
Samples
生物特質
資料擷取
32

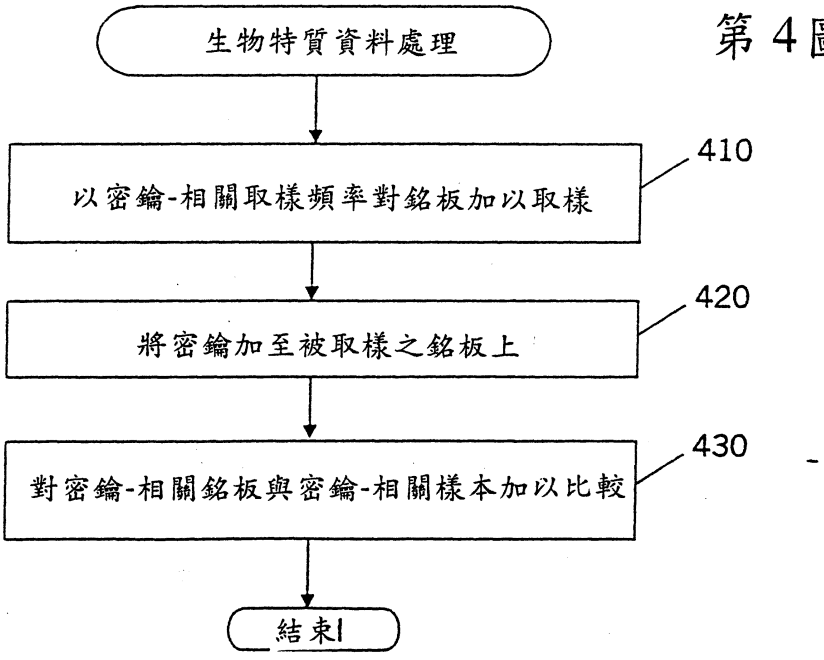
第 2 圖


伺服器
112
118
網頁伺服器
密鑰
相關樣本
142
比較模組
148
密鑰-相關銘板區塊
T1(k)
T2(k)
Tn(k)
140
銘板
T1
T2
Tn
124
伺服器
生物特質
文稿檔
網際網路
114
客戶端
110
網頁瀏覽器
密鑰
相關樣本
132
生物特質
資料獲取
116
122
客戶端
生物特質
嵌入檔

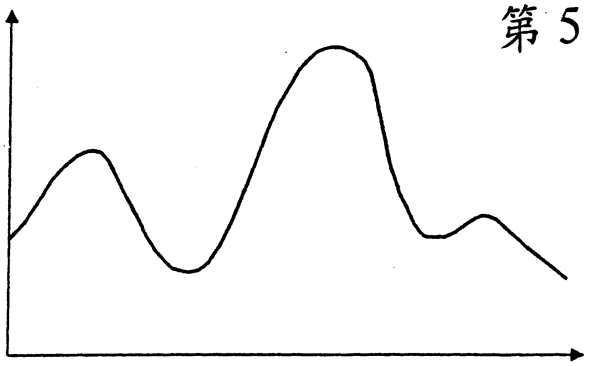
第 3 圖


生物特質資料傳輸
310
從伺服器傳輸一密鑰到客戶端
320
按照密鑰-相關樣本頻率
對生物特質特徵進行取樣
330
將密鑰加至被取樣之生物特質特徵上
340
將密鑰-相關樣本送至伺服器
結束

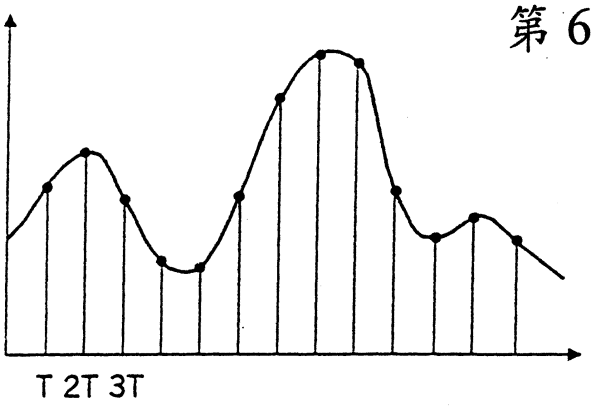
第 4 圖


生物特質資料處理
410
以密鑰-相關取樣頻率對銘板加以取樣
420
將密鑰加至被取樣之銘板上
430
對密鑰-相關銘板與密鑰-相關樣本加以比較
結束

第 5 圖



第 6 圖



第 7 圖