M569012

(19)中華民國智慧財產局

(12)新型說明書公告本 **(11)證書號數：TW M569012 U**

(45)公告日： 中華民國 107 (2018) 年 10 月 21 日

(21)申請案號：107205135 (22)申請日： 中華民國 107 (2018) 年 04 月 19 日

(51)Int. Cl.： ***G06K9/00 (2006.01)***

(71)申請人：中國信託金融控股股份有限公司(中華民國) CHINATRUST FINANCIAL HOLDING CO., LTD. (TW)

臺北市南港區經貿二路 168 號 27 樓、29 樓

(72)新型創作人：葉瑜君 YEH, YU-CHUN (TW)；王正男 WANG, CHENG NAN (TW)；郭明瓚 (TW)

(74)代理人：高玉駿；楊祺雄

(NOTE)備註： 相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

申請專利範圍項數：11 項 圖式數：3 共 27 頁

(54)名稱

利用生物特徵驗證電子文件的終端電子裝置

(57)摘要

一種利用生物特徵驗證電子文件的終端電子裝置，該終端電子裝置顯示一原始電子文件供一使用者簽署，該終端電子裝置取得該使用者的一簽名軌跡及至少一生物特徵，並向一憑證伺服器取得包含一公鑰及一私鑰的一金鑰對，且根據該至少一生物特徵及該私鑰產生一簽章值，並且將該簽章值及該簽名軌跡封裝成一第一資料，並以該私鑰對該至少一生物特徵加密而產生一第二資料，且將該第一資料合併於該原始電子文件中而產生一第三資料，再將該第一資料、該第二資料及該第三資料提供給一驗證伺服器。

指定代表圖：

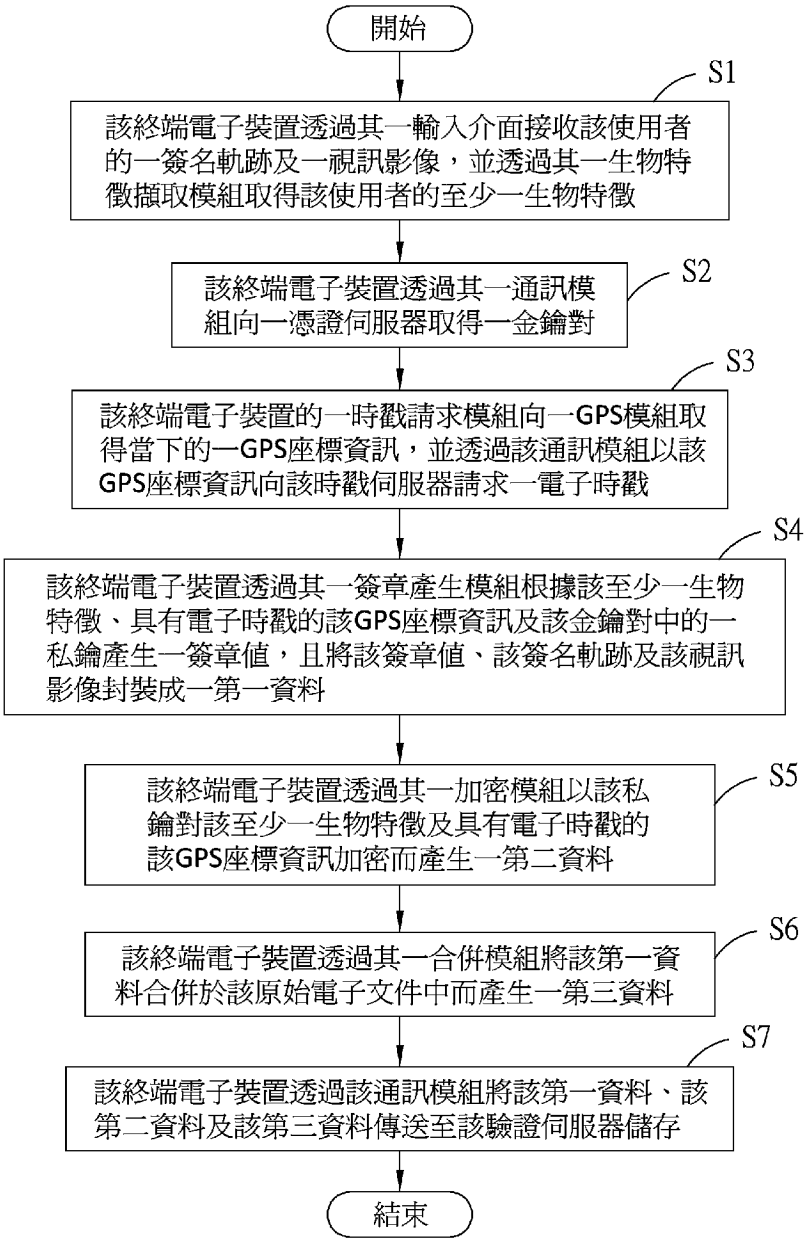

圖2

符號簡單說明：

100・・・終端電子裝置

200・・・網際網路

1・・・顯示單元

2・・・生物特徵擷取模組

3・・・GPS 模組

4・・・通訊模組

5・・・輸入介面

51・・・手寫輸入單元

52・・・影像擷取單元

6・・・處理單元

61・・・時戳請求模組

62・・・簽章產生模組

63・・・加密模組

64・・・合併模組

7・・・憑證伺服器

8・・・時戳伺服器

9・・・驗證伺服器

專利案號：107205135

公告本

M569012

【新型摘要】

【中文新型名稱】 利用生物特徵驗證電子文件的終端電子裝置

【中文】

一種利用生物特徵驗證電子文件的終端電子裝置，該終端電子裝置顯示一原始電子文件供一使用者簽署，該終端電子裝置取得該使用者的一簽名軌跡及至少一生物特徵，並向一憑證伺服器取得包含一公鑰及一私鑰的一金鑰對，且根據該至少一生物特徵及該私鑰產生一簽章值，並且將該簽章值及該簽名軌跡封裝成一第一資料，並以該私鑰對該至少一生物特徵加密而產生一第二資料，且將該第一資料合併於該原始電子文件中而產生一第三資料，再將該第一資料、該第二資料及該第三資料提供給一驗證伺服器。

【指定代表圖】：圖（2）。

【代表圖之符號簡單說明】

100……終端電子裝置

200……網際網路

1…… 顯示單元

2……生物特徵擷取模組

3……GPS 模組

4……通訊模組

5……輸入介面

51……手寫輸入單元

【新型圖式】

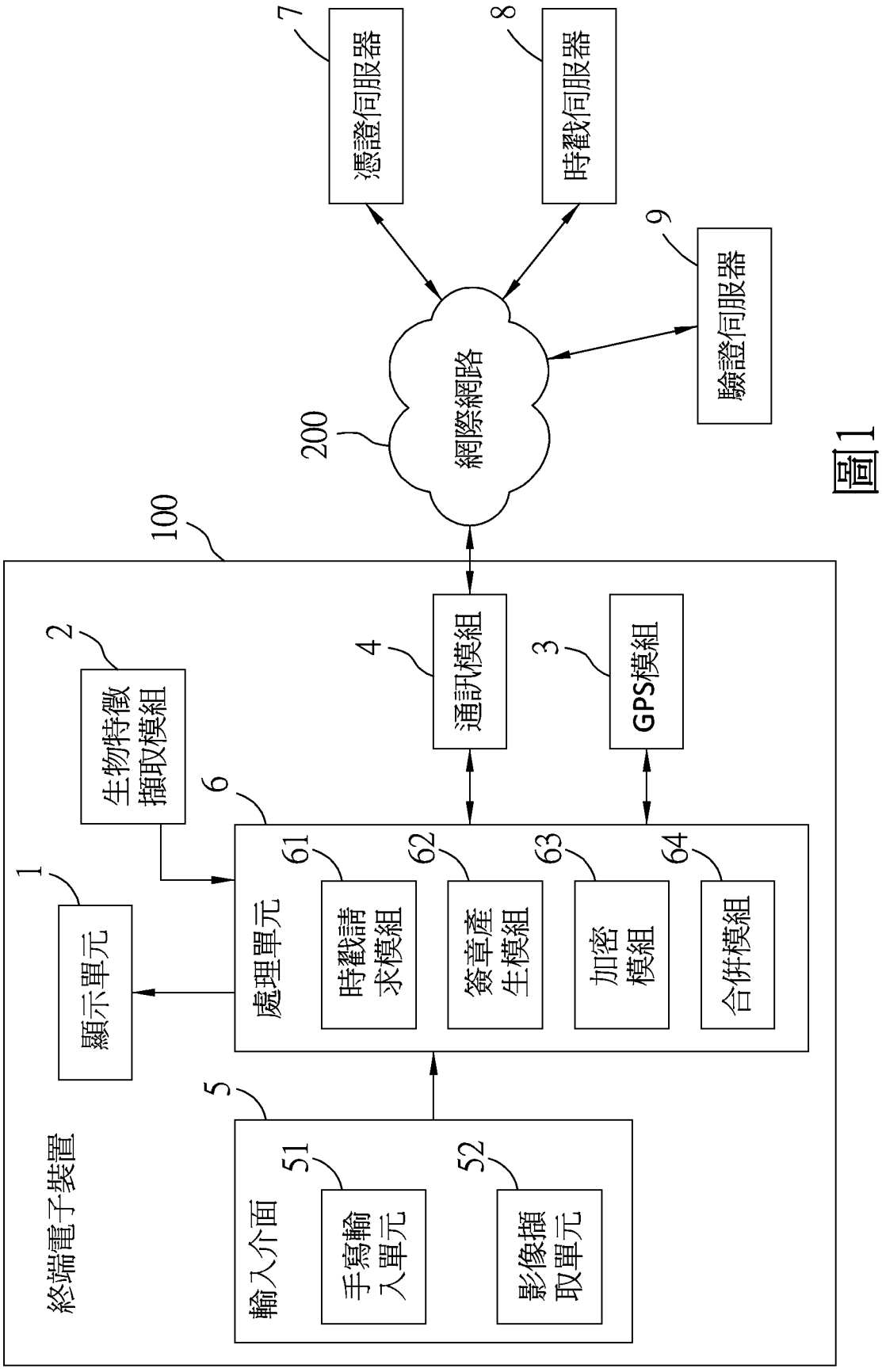
憑證伺服器
7
時戳伺服器
8
驗證伺服器
9
網際網路
200
100
通訊模組
4
GPS模組
3
生物特徵擷取模組
2
處理單元
6
61
時戳請求模組
62
簽章產生模組
63
加密模組
64
合併模組
顯示單元
1
輸入介面
5
51
手寫輸入單元
52
影像擷取單元
終端電子裝置

圖1

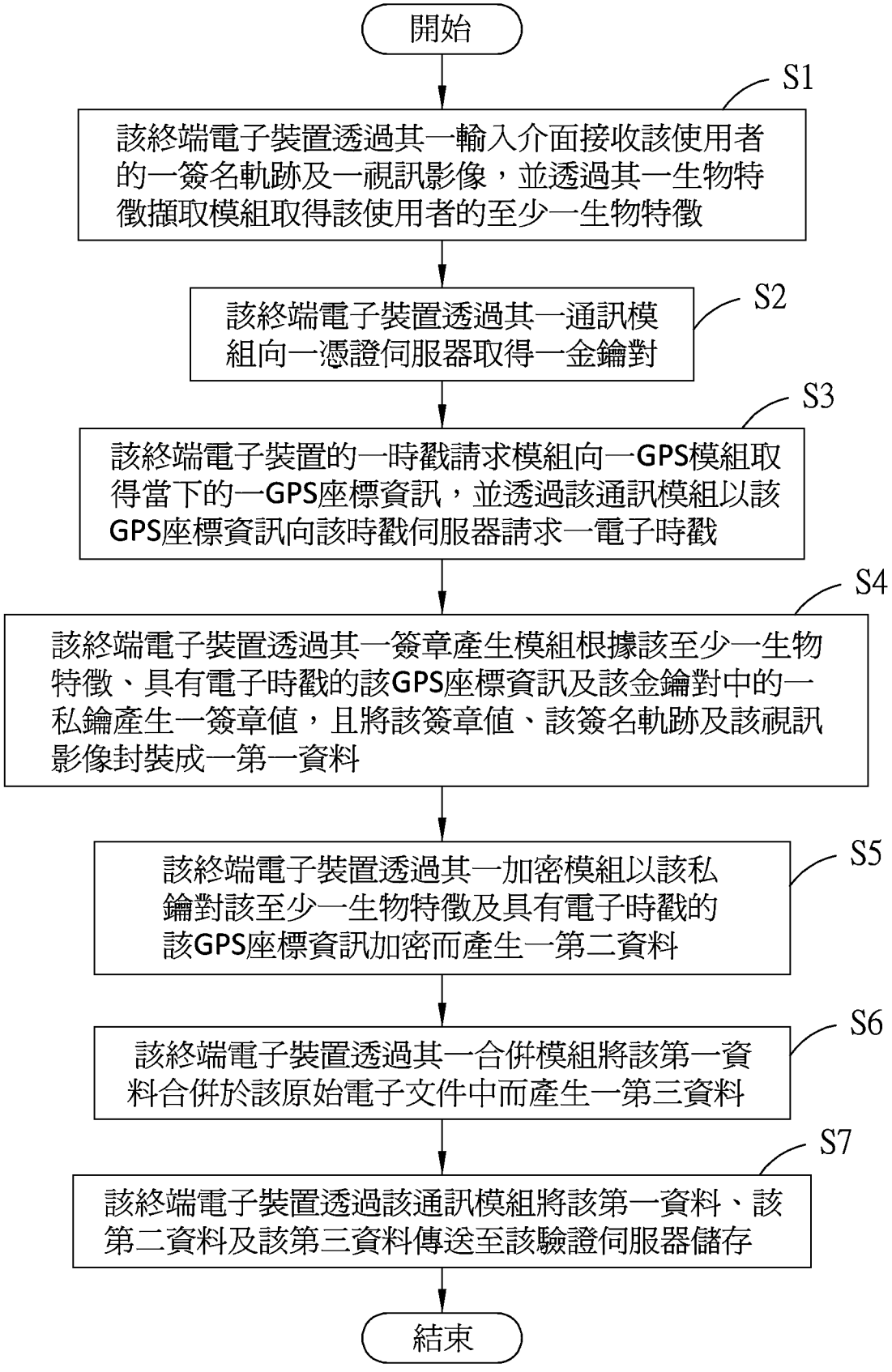
開始
S1
該終端電子裝置透過其一輸入介面接收該使用者的一簽名軌跡及一視訊影像，並透過其一生物特徵擷取模組取得該使用者的至少一生物特徵
S2
該終端電子裝置透過其一通訊模組向一憑證伺服器取得一金鑰對
S3
該終端電子裝置的一時戳請求模組向一GPS模組取得當下的一GPS座標資訊，並透過該通訊模組以該GPS座標資訊向該時戳伺服器請求一電子時戳
S4
該終端電子裝置透過其一簽章產生模組根據該至少一生物特徵、具有電子時戳的該GPS座標資訊及該金鑰對中的一私鑰產生一簽章值，且將該簽章值、該簽名軌跡及該視訊影像封裝成一第一資料
S5
該終端電子裝置透過其一加密模組以該私鑰對該至少一生物特徵及具有電子時戳的該GPS座標資訊加密而產生一第二資料
S6
該終端電子裝置透過其一合併模組將該第一資料合併於該原始電子文件中而產生一第三資料
S7
該終端電子裝置透過該通訊模組將該第一資料、該第二資料及該第三資料傳送至該驗證伺服器儲存
結束

圖2

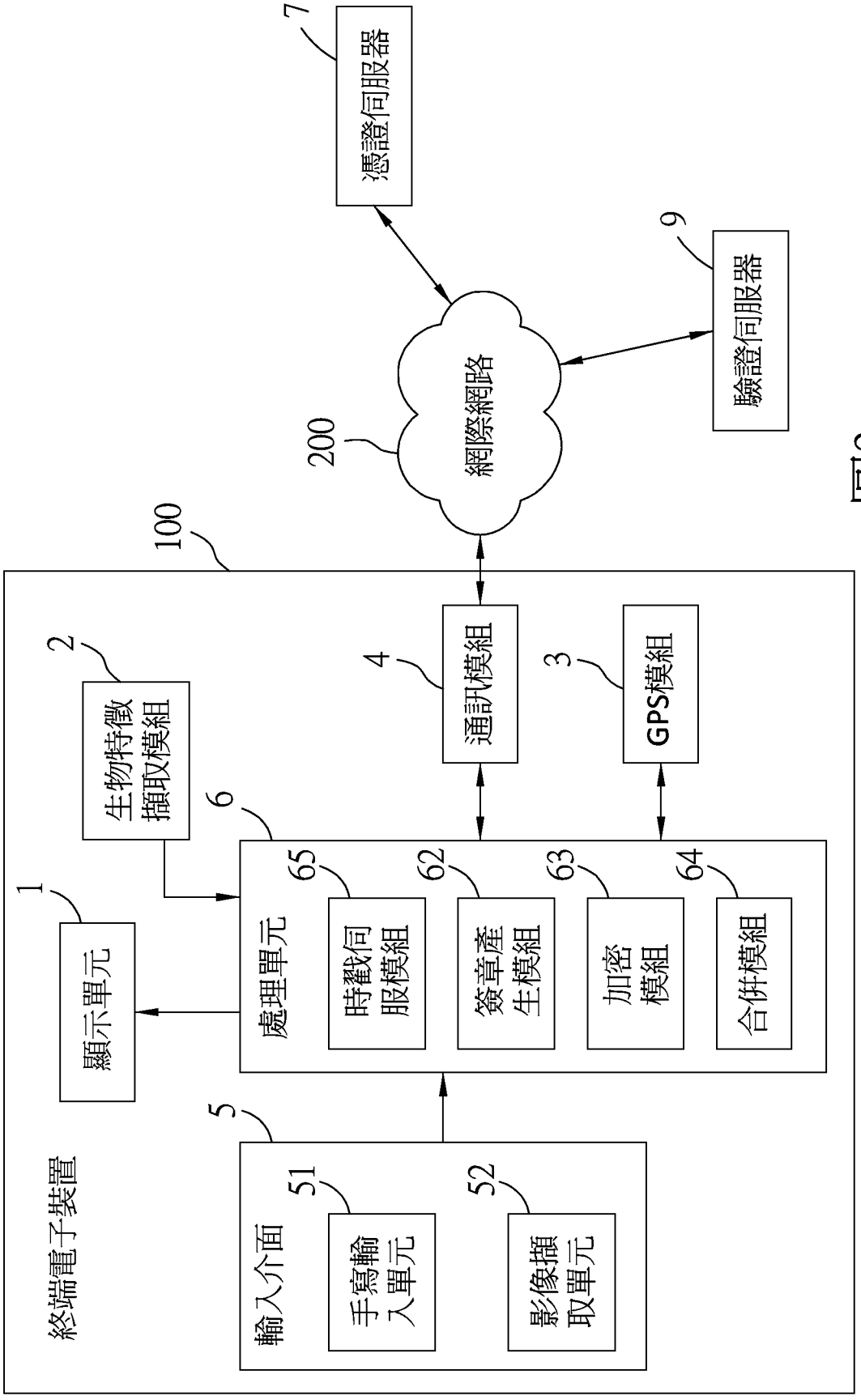
7
憑證伺服器
9
驗證伺服器
200
網際網路
100
2
生物特徵擷取模組
4
通訊模組
3
GPS模組
6
1
顯示單元
處理單元
65
時戳伺服模組
62
簽章產生模組
63
加密模組
64
合併模組
5
終端電子裝置
輸入介面
51
手寫輸入單元
52
影像擷取單元

圖3

公告本

【新型摘要】

【中文新型名稱】 利用生物特徵驗證電子文件的終端電子裝置

【中文】

一種利用生物特徵驗證電子文件的終端電子裝置，該終端電子裝置顯示一原始電子文件供一使用者簽署，該終端電子裝置取得該使用者的一簽名軌跡及至少一生物特徵，並向一憑證伺服器取得包含一公鑰及一私鑰的一金鑰對，且根據該至少一生物特徵及該私鑰產生一簽章值，並且將該簽章值及該簽名軌跡封裝成一第一資料，並以該私鑰對該至少一生物特徵加密而產生一第二資料，且將該第一資料合併於該原始電子文件中而產生一第三資料，再將該第一資料、該第二資料及該第三資料提供給一驗證伺服器。

【指定代表圖】：圖（2）。

【代表圖之符號簡單說明】

100……終端電子裝置

200……網際網路

1…… 顯示單元

2……生物特徵擷取模組

3……GPS 模組

4……通訊模組

5……輸入介面

51……手寫輸入單元

52……影像擷取單元

6 ……處理單元

61……時戳請求模組

62……簽章產生模組

63……加密模組

64……合併模組

7……憑證伺服器

8……時戳伺服器

9……驗證伺服器

【新型說明書】

【中文新型名稱】 利用生物特徵驗證電子文件的終端電子裝置

【技術領域】

【0001】 本新型是有關於一種電子文件驗證裝置，特別是指一種利用生物特徵驗證電子文件的終端電子裝置。

【先前技術】

【0002】現行的金融交易涉及需要客戶本人親自簽署交易相關文件的業務時，大多需要客戶親臨金融單位的櫃檯辦理，或者由銀行人員親訪客戶並完成親晤親簽作業，以鑑別客戶本人的真實身分並確認客戶本人的交易意願。然而上述做法受限於銀行營業時間，以致無法即時提供滿足客戶需求的金融服務。

【0003】因此，為了能即時提供滿足客戶需求的金融服務，現行一種電子交易方式能讓金融單位與客戶端透過約定機制進行遠距電子化交易指示。但這種交易方式只能間接地識別客戶身分，並無法鑑別提出交易指示的對象身分的真實性及其不可否認性。

【新型內容】

【0004】 因此，本新型之目的，即在提供一種利用生物特徵驗證電子文件的終端電子裝置，其能讓驗證單位藉由驗證根據生物特徵產生的簽章值，鑑別電子文件的署名者身分的真實性及其不可否

認性。

【0005】 於是，本新型利用生物特徵驗證電子文件的終端電子裝置，能與一憑證伺服器及一驗證伺服器通訊，且該終端電子裝置顯示一原始電子文件供一使用者簽署；該終端電子裝置包括：一顯示單元；一生物特徵擷取模組；一通訊模組；一輸入介面；及一處理單元，其與該顯示單元、該生物特徵擷取模組、該通訊模組及該輸入介面電耦接，而令該顯示單元顯示該原始電子文件，並令該輸入介面接受該使用者輸入的一簽名軌跡以在該原始電子文件上簽名，且令該生物特徵擷取模組取得該使用者的至少一生物特徵，並透過該通訊模組向該憑證伺服器取得包含一公鑰及一私鑰的一金鑰對；該處理單元的一簽章產生模組根據該至少一生物特徵及該私鑰產生一簽章值，且將該簽章值及該簽名軌跡封裝成一第一資料，該處理單元的一加密模組並以該私鑰對該至少一生物特徵加密而產生一第二資料，並且該處理單元的一合併模組將該第一資料合併於該原始電子文件中而產生一第三資料，該處理單元再將該第一資料、該第二資料及該第三資料透過該通訊模組提供給該驗證伺服器。

【0006】 在本新型的一些實施態樣中，該驗證伺服器能向該憑證伺服器或該終端電子裝置取得該金鑰對，並具有與該終端電子裝置的該處理單元中的該簽章產生模組相同的一簽章產生模組，且該

驗證伺服器藉由該金鑰對中的該公鑰對該第二資料解密，而取得該至少一生物特徵，並透過其中的該簽章產生模組根據解密取得的該至少一生物特徵及該金鑰對中的該私鑰產生一待驗證簽章值，並比對該待驗證簽章值與該第一資料中的該簽章值是否相同，以驗證該第一資料中的該簽名軌跡的真實性，並根據該簽名軌跡的真實性確認該第三資料的不可否認性。

【0007】 在本新型的一些實施態樣中，該輸入介面包含一手寫輸入單元及一影像擷取單元，該手寫輸入單元供手寫以輸入該簽名軌跡，該影像擷取單元擷取該使用者的一視訊影像，且該處理單元將該簽章值、該簽名軌跡及該視訊影像封裝成該第一資料；藉此，該驗證伺服器藉由比對該待驗證簽章值與該第一資料中的該簽章值是否相同，以驗證該第一資料中的該簽名軌跡及該視訊影像的真實性，而根據該簽名軌跡及該視訊影像的真實性確認該第三資料的不可否認性。

【0008】 在本新型的一些實施態樣中，該終端電子裝置還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並且該處理單元的一時戳請求模組還透過該通訊模組向一時戳伺服器請求一電子時戳，或者以該GPS座標資訊向該時戳伺服器請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；且該處理單元的該簽章產生模組根據該至少一生物特徵、該私鑰以及該

GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該簽章值，該處理單元的該加密模組並以該私鑰對該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一用來產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該公鑰對該第二資料解密，而取得該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一，並透過該簽章產生模組根據該私鑰及解密取得的該至少一生物特徵、該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該待驗證簽章值。

【0009】 或者，在本新型的一些實施態樣中，該終端電子裝置包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並且該處理單元的一時戳請求模組還透過該通訊模組向一時戳伺服器請求一電子時戳，或者以該GPS座標資訊向該時戳伺服器請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；且該處理單元的該簽章產生模組根據該至少一生物特徵、該私鑰以及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該簽章值，且將該簽章值、該簽名軌跡及該視訊影像封裝成該第一資料，該處理單元的該加密模組並以該私鑰對該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時

戳的該GPS座標資訊三者其中之一用來產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該公鑰對該第二資料解密，而取得該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一，並透過該簽章產生模組根據該私鑰及解密取得的該至少一生物特徵、該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該待驗證簽章值。

【0010】 或者，在本新型的一些實施態樣中，該處理單元還包括一時戳伺服模組，且該處理單元還令該時戳伺服模組產生一電子時戳，或者該終端電子裝置還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並以該GPS座標資訊向該時戳伺服模組請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；並且該處理單元的該簽章產生模組根據該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該簽章值，且將該簽章值及該簽名軌跡封裝成該第一資料，而且該處理單元的該加密模組以該私鑰對該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊其中之一用以產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該金鑰對中的該公鑰對該第二資料解密，而取得該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊，並透過該簽章產生模組根據解密

取得的該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該待驗證簽章值。

【0011】 或者，在本新型的一些實施態樣中，該處理單元還包括一時戳伺服模組，且該處理單元還令該時戳伺服模組產生一電子時戳，或者該終端電子裝置還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並以該GPS座標資訊向該時戳伺服模組請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；並且該處理單元的該簽章產生模組根據該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該簽章值，且將該簽章值、該簽名軌跡及該視訊影像封裝成該第一資料；而且該處理單元的該加密模組以該私鑰對該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊其中之一用以產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該金鑰對中的該公鑰對該第二資料解密，而取得該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊，並透過該簽章產生模組根據解密取得的該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該待驗證簽章值。

【0012】 在本新型的一些實施態樣中，該處理單元是執行一安裝於該終端電子裝置中的應用程式，該應用程式包含該時戳請求模組、該簽章產生模組、該加密模組及該合併模組。

【0013】 或者，在本新型的一些實施態樣中，該處理單元是執行一安裝於該終端電子裝置中的應用程式，該應用程式包含該時戳伺服模組、該簽章產生模組、該加密模組及該合併模組。

【0014】 或者，在本新型的一些實施態樣中，該時戳請求模組、該簽章產生模組、該加密模組及該合併模組是燒錄在該處理單元中的韌體。

【0015】 或者，在本新型的一些實施態樣中，該時戳伺服模組、該簽章產生模組、該加密模組及該合併模組是燒錄在該處理單元中的韌體。

【0016】 本新型之功效在於：藉由根據該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)及該私鑰產生該簽章值，且將該簽章值及該簽名軌跡(及該視訊影像)封裝成該第一資料，並以該私鑰對該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)加密而產生該第二資料，並將該第一資料合併於該原始電子文件中而產生該第三資料，且將該第一資料、第二資料及第三資料記錄在該驗證伺服器中，藉此，該驗證伺服器能藉由對該第二資料解密而獲得該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)，並根據該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)及該私鑰產生該待

驗證簽章值，並比對該待驗證簽章值與該第一資料中的該簽章值是否一致，而判定第一資料中的該簽名軌跡(及該視訊影像)的真實性，並在驗證第一資料中的該簽名軌跡(及該視訊影像)的真實性之後，即可根據第一資料確認第三資料(即完成數位簽章的電子文件)確實為簽署人表示同意及不可否認的文件。

【圖式簡單說明】

【0017】 本新型之其他的特徵及功效，將於參照圖式的實施方式中清楚地顯示，其中：

圖 1 是本新型利用生物特徵驗證電子文件的終端電子裝置的一實施例的主要電路及模組方塊圖；

圖 2 是本實施例的主要流程圖；及

圖 3 是本新型利用生物特徵驗證電子文件的終端電子裝置的另一實施例的主要電路及模組方塊圖。

【實施方式】

【0018】 在本新型被詳細描述之前，應當注意在以下的說明內容中，類似的元件是以相同的編號來表示。

【0019】 參閱圖 1，是本新型利用生物特徵驗證電子文件的終端電子裝置(以下簡稱終端電子裝置)的一實施例的主要電路及模組方塊，用以執行如圖 2 所示的一驗證電子文件流程。該終端電子裝置 100 可以是使用者所持有的行動電話、平板電腦、個人電腦，或

者是金融機構設置的可供用戶直接操作以購買/賣出理財產品、申請貸款、預借現金及提款...等多種金融服務的金融服務終端設備，且如圖 2 所示，該終端電子裝置 100 主要包括一顯示單元 1、一生物特徵擷取模組 2、一 GPS 模組 3、一通訊模組 4、一輸入介面 5 及一與前述元件電耦接的處理單元 6。

【0020】 其中，顯示單元 1 在本實施例中用以顯示一供一使用者閱覽並簽署的原始電子文件(圖未示)；該生物特徵擷取模組 2 用以取得使用者的至少一生物特徵，例如使用者的臉部、聲音、指靜脈、指紋等其中至少一者，但不以此為限。該 GPS 模組 3 用以取得該終端電子裝置 1 當下的一 GPS 座標資訊。該通訊模組 4 用以透過網際網路 200 與一憑證伺服器 7、一時戳伺服器 8 及一驗證伺服器 9 通訊；該輸入介面 5 在本實施例中包含一手寫輸入單元 51 及一影像擷取單元 52，該手寫輸入單元 51 可以是例如一手寫板、一電子簽名板或者與該顯示單元 1 整合在一起的一觸控顯示面板等，但不以此為限；該影像擷取單元 52 可以是一照相機或攝影機，用以取得該使用者的一視訊影像。

【0021】 該處理單元 6 在本實施例中是執行預先安裝於該終端電子裝置 100 中的一應用程式而完成本實施例的方法，且如圖 2 所示，該應用程式包含一時戳請求模組 61、一簽章產生模組 62、一加密模組 63 及一合併模組 64。當然該等模組 61~64 也可以韌

體方式實現而被燒錄在該處理單元 6 中，並不以軟體為限。

【0022】 因此，當使用者要在原始電子文件上簽名而透過手寫輸入單元51輸入其一簽名軌跡時，該處理單元6將收到由該手寫輸入單元51傳來的該簽名軌跡，此時，如圖2的步驟S1，該處理單元6控制該影像擷取單元52取得該使用者的該視訊影像，例如該使用者的臉部影像，並控制該生物特徵擷取模組2取得該使用者的至少一生物特徵。並且，如圖2的步驟S2，該處理單元6透過該通訊模組4向該憑證伺服器7要求提供包含一公鑰及一私鑰的一金鑰對(憑證)；而且如圖2的步驟S3，該處理單元6的該時戳請求模組61向該GPS模組3取得當下的該GPS座標資訊，並透過該通訊模組4傳送該GPS座標資訊給該時戳伺服器8，向該時戳伺服器8請求一電子時戳。因此，該時戳伺服器8將在該GPS座標資訊押上電子時戳，並記錄具有電子時戳的該GPS座標資訊後，透過該通訊模組4回傳具有電子時戳的該GPS座標資訊給該處理單元6。值得一提的是，上述步驟S1、S2、S3並無先後之分，也可以同時執行或對調順序執行。

【0023】 然後，如圖2的步驟S4，該處理單元6的該簽章產生模組62根據該至少一生物特徵、具有電子時戳的該GPS座標資訊及該私鑰產生一簽章值，且將該簽章值、該簽名軌跡及該視訊影像封裝成一第一資料；具體而言，該簽章產生模組62會將該至少一生物特

徵、具有電子時戳的該GPS座標資訊及該私鑰以不可逆的雜湊摘要演算法（Digest Hash）(或稱雜湊函數)，例如 SHA1 或 MD5進行演算，產生一雜湊摘要（Digest），即本實施例所稱的該簽章值(或稱數位指紋)，再將該簽章值、該簽名軌跡及該視訊影像封裝成具有一標準資料格式，例如 PKCS#7的該第一資料。

【0024】 接著，如圖2的步驟S5，該處理單元6的該加密模組63以該私鑰對該至少一生物特徵及具有電子時戳的該GPS座標資訊進行非對稱式加密而產生一第二資料；然後，如圖2的步驟S6，該處理單元6的該合併模組64將該第一資料合併於該原始電子文件中而產生一第三資料，即完成數位簽章的電子文件。最後，如圖2的步驟S7，該處理單元6透過該通訊模組4將該第一資料、該第二資料及該第三資料傳送至該驗證伺服器9，即完成該原始電子文件及其數位簽章的儲存作業。

【0025】 而且，該驗證伺服器9具有與該終端電子裝置相同的該簽章產生模組62。藉此，當該驗證伺服器9之後(或日後)欲驗證該原始電子文件的數位簽章真實性及其簽署人的表示同意及不可否認性時，該驗證伺服器9能向該憑證伺服器7(或該終端電子裝置100)取得該金鑰對，並藉由該金鑰對中的公鑰及預設的一解密演算法，對該第二資料進行非對稱式解密，而從中取得該至少一生物特徵及具有電子時戳的該GPS座標資訊，並利用該簽章產生模組62

根據解密取得的該至少一生物特徵、具有電子時戳的該GPS座標資訊及該金鑰對中的私鑰產生一待驗證簽章值，並比對該待驗證簽章值與該第一資料中的該簽章值是否相同，若是，即代表該第一資料中的該簽名軌跡及該視訊影像在傳送過程中沒有被竄改，而具有其真實性。

【0026】 因此，在驗證第一資料中的該簽名軌跡及該視訊影像的真實性之後，即可根據第一資料確認第三資料(即完成數位簽章的電子文件)確實為簽署人表示同意及不可否認的文件，而具有不可否認性。

【0027】 值得一提的是，本實施例亦可由該時戳請求模組61直接向該時戳伺服器8請求一電子時戳，且該簽章產生模組62根據該至少一生物特徵、該電子時戳及該私鑰產生該簽章值，且該加密模組63以該私鑰對該至少一生物特徵及該電子時戳加密而產生該第二資料；因此，該驗證伺服器9藉由該金鑰對中的該公鑰對該第二資料解密後，將取得該至少一生物特徵及該電子時戳，並透過該簽章產生模組62根據解密取得的該至少一生物特徵、該電子時戳及該私鑰產生該待驗證簽章值；此外，本實施例亦可因應其他應用上的需求而省略擷取視訊影像的步驟以及/或者省略上述的時戳請求模組61(即省略上述的步驟S3)，同樣能達到本案上述的目的。

【0028】 此外，本實施例未使用上述的時戳請求模組61時，在

步驟S4中，該簽章產生模組62即根據該至少一生物特徵、該GPS座標資訊及該私鑰產生該簽章值，且在步驟S5中，該加密模組以該私鑰對該至少一生物特徵及該GPS座標資訊加密而產生該第二資料；因此，該驗證伺服器9藉由該金鑰對中的該公鑰對該第二資料解密後，將取得該至少一生物特徵及該GPS座標資訊，並透過該簽章產生模組62根據解密取得的該至少一生物特徵、該GPS座標資訊及該私鑰產生該待驗證簽章值。

【0029】 或者，在其他的實施態樣中，亦可省略上述的該時戳請求模組61(即省略上述的步驟S3)，亦即不透過該時戳請求模組61向該時戳伺服器8取得電子時戳，而是如圖3所示，令該處理單元6還包含一時戳伺服模組65，該時戳伺服模組65能取代該時戳伺服器8而具有產生電子時戳的功能。因此，在步驟S1中，該處理單元6還令該時戳伺服模組65產生一電子時戳，或者以該GPS座標資訊向該時戳伺服模組65請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊，且在步驟S4中，該簽章產生模組62根據該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該簽章值，而且在步驟S5中，該加密模組63以該私鑰對該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊加密而產生該第二資料；因此，該驗證伺服器9藉由該金鑰對中的該公鑰對該第二資料解密，將取得該至少一生物特徵及該電子時戳或

具有電子時戳的該GPS座標資訊，並透過該簽章產生模組62根據解密取得的該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該待驗證簽章值。

【0030】 綜上所述，上述實施例藉由簽章產生模組62根據該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)及該私鑰產生該簽章值，且將該簽章值及該簽名軌跡(及該視訊影像)封裝成該第一資料，並藉由加密模組63以該私鑰對該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)加密而產生該第二資料，並藉由該合併模組64將該第一資料合併於該原始電子文件中而產生該第三資料，且將該第一資料、第二資料及第三資料記錄在該驗證伺服器9中，藉此，該驗證伺服器9能藉由對該第二資料解密而獲得該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)，並根據該至少一生物特徵(及該GPS座標資訊、該電子時戳或具有電子時戳的該GPS座標資訊)及該私鑰產生該待驗證簽章值，並比對該待驗證簽章值與該第一資料中的該簽章值是否一致，而判定第一資料中的該簽名軌跡(及該視訊影像)的真實性，並在驗證第一資料中的該簽名軌跡(及該視訊影像)的真實性之後，即可根據第一資料確認第三資料(即完成數位簽章的電子文件)確實為簽署人表示同意及不可否認的文件，而達到本新型之功效與

目的。

【0031】 惟以上所述者，僅為本新型之實施例而已，當不能以此限定本新型實施之範圍，凡是依本新型申請專利範圍及專利說明書內容所作之簡單的等效變化與修飾，皆仍屬本新型專利涵蓋之範圍內。

【符號說明】

【0032】

S1~S7……步驟

100……終端電子裝置

200……網際網路

1…… 顯示單元

2……生物特徵擷取模組

3……GPS 模組

4……通訊模組

5……輸入介面

51……手寫輸入單元

52……影像擷取單元

6 ……處理單元

61……時戳請求模組

62……簽章產生模組

63……加密模組

64……合併模組

65……時戳伺服模組

7……憑證伺服器

8……時戳伺服器

9……驗證伺服器

【新型申請專利範圍】

【第1項】 一種利用生物特徵驗證電子文件的終端電子裝置，能與一憑證伺服器及一驗證伺服器通訊，且該終端電子裝置顯示一原始電子文件供一使用者簽署；該終端電子裝置包括：

一顯示單元；

一生物特徵擷取模組；

一通訊模組；

一輸入介面；及

一處理單元，其與該顯示單元、該生物特徵擷取模組、該通訊模組及該輸入介面電耦接，而令該顯示單元顯示該原始電子文件，並令該輸入介面接受該使用者輸入的一簽名軌跡以在該原始電子文件上簽名，且令該生物特徵擷取模組取得該使用者的至少一生物特徵，並透過該通訊模組向該憑證伺服器取得包含一公鑰及一私鑰的一金鑰對；該處理單元的一簽章產生模組根據該至少一生物特徵及該私鑰產生一簽章值，且將該簽章值及該簽名軌跡封裝成一第一資料，該處理單元的一加密模組並以該私鑰對該至少一生物特徵加密而產生一第二資料，並且該處理單元的一合併模組將該第一資料合併於該原始電子文件中而產生一第三資料，該處理單元再將該第一資料、該第二資料及該第三資料透過該通訊模組提供給該驗證伺服器。

【第2項】 如請求項1所述利用生物特徵驗證電子文件的終端電子裝置，其中，該驗證伺服器能向該憑證伺服器或該終端電子裝置取得該金鑰對，並具有與該終端電子裝置的該處理單

元中的該簽章產生模組相同的一簽章產生模組，且該驗證伺服器藉由該金鑰對中的該公鑰對該第二資料解密，而取得該至少一生物特徵，並透過其中的該簽章產生模組根據解密取得的該至少一生物特徵及該金鑰對中的該私鑰產生一待驗證簽章值，並比對該待驗證簽章值與該第一資料中的該簽章值是否相同，以驗證該第一資料中的該簽名軌跡的真實性，並根據該簽名軌跡的真實性確認該第三資料的不可否認性。

【第3項】 如請求項2所述利用生物特徵驗證電子文件的終端電子裝置，其中該輸入介面包含一手寫輸入單元及一影像擷取單元，該手寫輸入單元供手寫以輸入該簽名軌跡，該影像擷取單元擷取該使用者的一視訊影像，且該處理單元將該簽章值、該簽名軌跡及該視訊影像封裝成該第一資料；藉此，該驗證伺服器藉由比對該待驗證簽章值與該第一資料中的該簽章值是否相同，以驗證該第一資料中的該簽名軌跡及該視訊影像的真實性，而根據該簽名軌跡及該視訊影像的真實性確認該第三資料的不可否認性。

【第4項】 如請求項2所述利用生物特徵驗證電子文件的終端電子裝置，還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並且該處理單元的一時戳請求模組還透過該通訊模組向一時戳伺服器請求一電子時戳，或者以該GPS座標資訊向該時戳伺服器請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；且該處理單元的該簽章產生模組根據該至少一生物特徵、該私鑰以及

該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該簽章值，該處理單元的該加密模組並以該私鑰對該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一用來產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該公鑰對該第二資料解密，而取得該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一，並透過該簽章產生模組根據該私鑰及解密取得的該至少一生物特徵、該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該待驗證簽章值。

【第5項】 如請求項3所述利用生物特徵驗證電子文件的終端電子裝置，還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並且該處理單元的一時戳請求模組還透過該通訊模組向一時戳伺服器請求一電子時戳，或者以該GPS座標資訊向該時戳伺服器請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；且該處理單元的該簽章產生模組根據該至少一生物特徵、該私鑰以及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該簽章值，且將該簽章值、該簽名軌跡及該視訊影像封裝成該第一資料，該處理單元的該加密模組並以該私鑰對該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一用來產生該簽章值者加密而產生該第二資料；藉

此，該驗證伺服器藉由該公鑰對該第二資料解密，而取得該至少一生物特徵及該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一，並透過該簽章產生模組根據該私鑰及解密取得的該至少一生物特徵、該GPS座標資訊、該電子時戳和具有電子時戳的該GPS座標資訊三者其中之一產生該待驗證簽章值。

【第6項】 如請求項2所述利用生物特徵驗證電子文件的終端電子裝置，其中該處理單元還包括一時戳伺服模組，且該處理單元還令該時戳伺服模組產生一電子時戳，或者該終端電子裝置還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並以該GPS座標資訊向該時戳伺服模組請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；並且該處理單元的該簽章產生模組根據該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該簽章值，且將該簽章值及該簽名軌跡封裝成該第一資料，而且該處理單元的該加密模組以該私鑰對該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊其中之一用以產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該金鑰對中的該公鑰對該第二資料解密，而取得該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊，並透過該簽章產生模組根據解密取得的該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該待驗證簽章值。

【第7項】 如請求項3所述利用生物特徵驗證電子文件的終端電子裝置，其中該處理單元還包括一時戳伺服模組，且該處理單元還令該時戳伺服模組產生一電子時戳，或者該終端電子裝置還包括一GPS模組，且該處理單元還透過該GPS模組取得當下的一GPS座標資訊，並以該GPS座標資訊向該時戳伺服模組請求一電子時戳，使回傳具有電子時戳的該GPS座標資訊；並且該處理單元的該簽章產生模組根據該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該簽章值，且將該簽章值、該簽名軌跡及該視訊影像封裝成該第一資料；而且該處理單元的該加密模組以該私鑰對該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊其中之一用以產生該簽章值者加密而產生該第二資料；藉此，該驗證伺服器藉由該金鑰對中的該公鑰對該第二資料解密，而取得該至少一生物特徵及該電子時戳或具有電子時戳的該GPS座標資訊，並透過該簽章產生模組根據解密取得的該至少一生物特徵、該電子時戳或具有電子時戳的該GPS座標資訊及該私鑰產生該待驗證簽章值。

【第8項】 如請求項4或5所述利用生物特徵驗證電子文件的終端電子裝置，其中該處理單元是執行一安裝於該終端電子裝置中的應用程式，該應用程式包含該時戳請求模組、該簽章產生模組、該加密模組及該合併模組。

【第9項】 如請求項6或7所述利用生物特徵驗證電子文件的終端電子裝置，其中該處理單元是執行一安裝於該終端電子裝置

中的應用程式，該應用程式包含該時戳伺服模組、該簽章產生模組、該加密模組及該合併模組。

【第10項】如請求項4或5所述利用生物特徵驗證電子文件的終端電子裝置，其中該時戳請求模組、該簽章產生模組、該加密模組及該合併模組是燒錄在該處理單元中的韌體。

【第11項】如請求項6或7所述利用生物特徵驗證電子文件的終端電子裝置，其中該時戳伺服模組、該簽章產生模組、該加密模組及該合併模組是燒錄在該處理單元中的韌體。