I455562

(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 I455562 B**

(45)公告日： 中華民國 103 (2014) 年 10 月 01 日

(21)申請案號：100148877 (22)申請日： 中華民國 100 (2011) 年 12 月 27 日

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

(71)申請人：捷而思股份有限公司 (中華民國) JRSYS INTERNATIONAL CORP. (TW)
臺北市中山區中山北路 3 段 29 號 10 樓 2 室

(72)發明人：吳建東 WU, JIANN DONG (TW) ；林岱宏 LIN, TAI HUNG (TW) ；陳嘉宏 CHEN, JIA HONG (TW) ；洪伯岳 HUNG, PO YUEH (TW) ；沈岩毅 SHEN, YAN YI (TW) ；張聰裕 CHANG, TSUNG YU (TW)

(74)代理人：施志豪；郭仁智

(56)參考文獻：

TW 525072 TW 200826597A

審查人員：周官緯

申請專利範圍項數：15 項 圖式數：5 共 31 頁

(54)名稱

使用圖形碼的雙通道電子簽章系統及相關的方法和電腦程式產品

DUAL-CHANNEL ELECTRONIC SIGNATURE SYSTEM USING IMAGE CODES AND RELATED METHOD AND COMPUTER PROGRAM PRODUCT

(57)摘要

本專利提出的雙通道電子簽章系統之一，包含有：一簽章核對伺服器；一簽章請求者裝置，用於計算與一目標文件的內容對應的特徵值、對待簽章的該特徵值與一傳送目的地信息進行編碼以產生一第一圖形、並輸出該第一圖形；以及一手持裝置，用於擷取並解碼該第一圖形的影像以取得該特徵值、對該特徵值進行電子簽章以產生一簽章資料、對該簽章資料進行編碼以產生一第二圖形、並將該第二圖形傳送至一目的網址；其中若該第二圖形所包含的該簽章資料通過該簽章核對伺服器的核對程序，則該簽章核對伺服器會將與該第二圖形相對應的核對圖形傳送至該簽章請求者裝置。

A dual-channel electronic signature system is disclosed, having a signature verification server; a signature requester device for calculating a characteristic value related to the content of a target document, encoding the characteristic value and a destination message to generate a first graph, and outputting the first graph; and a hand-held device for capturing and decoding the image of the first graph to obtain the characteristic value, performing an electronic signature operation on the characteristic value to generate a signature data, encoding the signature data to generate a second graph, and transmitting the second graph to a destination network address; wherein if the signature data contained in the second graph passed a verification procedure of the signature verification server, the signature verification server transmits a verification graph corresponding to the second graph to the signature requester device.

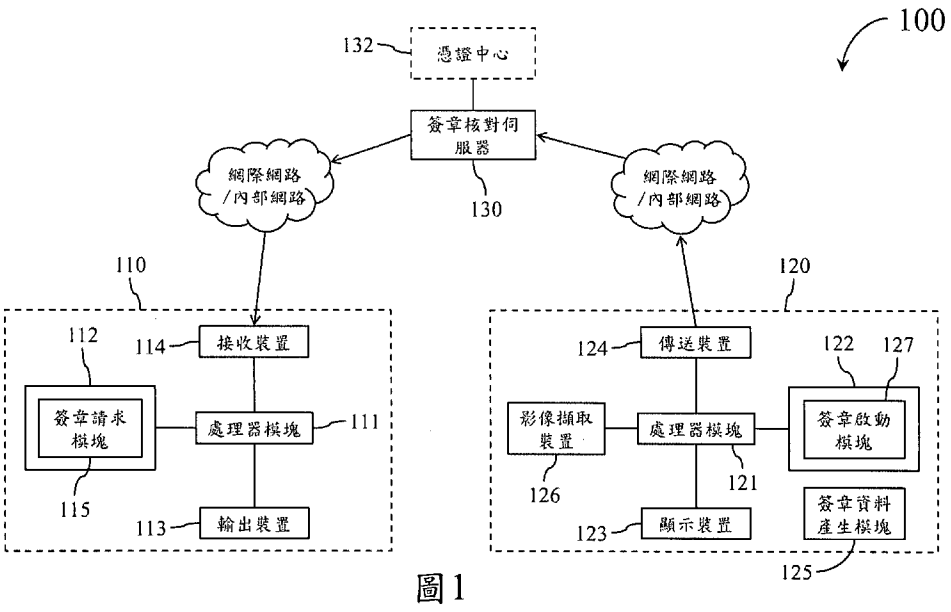

圖1

100・・・雙通道電子簽章系統

110・・・簽章請求者裝置

111、121・・・處理器模塊

112、122・・・儲存裝置

113・・・輸出裝置

114・・・接收裝置

115・・・簽章請求模塊

120・・・手持裝置

123・・・顯示裝置

124・・・傳送裝置

125・・・簽章資料產生模塊

126・・・影像擷取裝置

127・・・簽章啟動模塊

130・・・簽章核對伺服器

132・・・憑證中心

I455562 專利案號：100148877

公告本

103年05月28日 修正替換頁

申請日：100、12、27

IPC分類：H04L 9/32 (2006.01)

【發明摘要】

【中文發明名稱】 使用圖形碼的雙通道電子簽章系統及相關的方法和電腦程式產品

【英文發明名稱】 DUAL-CHANNEL ELECTRONIC SIGNATURE SYSTEM USING IMAGE CODES AND RELATED METHOD AND COMPUTER PROGRAM PRODUCT

【中文】

本專利提出的雙通道電子簽章系統之一，包含有：一簽章核對伺服器；一簽章請求者裝置，用於計算與一目標文件的內容對應的特徵值、對待簽章的該特徵值與一傳送目的地信息進行編碼以產生一第一圖形、並輸出該第一圖形；以及一手持裝置，用於擷取並解碼該第一圖形的影像以取得該特徵值、對該特徵值進行電子簽章以產生一簽章資料、對該簽章資料進行編碼以產生一第二圖形、並將該第二圖形傳送至一目的網址；其中若該第二圖形所包含的該簽章資料通過該簽章核對伺服器的核對程序，則該簽章核對伺服器會將與該第二圖形相對應的核對圖形傳送至該簽章請求者裝置。

【英文】

A dual-channel electronic signature system is disclosed, having a signature verification server; a signature requester device for calculating a characteristic value related to the content of a target document, encoding the characteristic value and a destination message to generate a first graph, and outputting the first graph; and a hand-held device for capturing and decoding the image of the first graph to obtain the characteristic value, performing an electronic signature operation on the characteristic value to generate a signature data, encoding the signature data to generate a second graph, and transmitting the second graph to a destination network

address; wherein if the signature data contained in the second graph passed a verification procedure of the signature verification server, the signature verification server transmits a verification graph corresponding to the second graph to the signature requester device.

【指定代表圖】 圖1

【代表圖之符號簡單說明】

100 雙通道電子簽章系統

110 簽章請求者裝置

111、121 處理器模塊

112、122 儲存裝置

113 輸出裝置

114 接收裝置

115 簽章請求模塊

120 手持裝置

123 顯示裝置

124 傳送裝置

125 簽章資料產生模塊

126 影像擷取裝置

127 簽章啓動模塊

130 簽章核對伺服器

132 憑證中心

【特徵化學式】

無

103年05月28日 修正替換頁

【發明說明書】

【中文發明名稱】 使用圖形碼的雙通道電子簽章系統及相關的方法和電腦程式產品

【英文發明名稱】 DUAL-CHANNEL ELECTRONIC SIGNATURE SYSTEM USING IMAGE CODES AND RELATED METHOD AND COMPUTER PROGRAM PRODUCT

【技術領域】

【0001】 本發明有關電子簽章技術，尤指一種使用影像碼的雙通道電子簽章系統及相關的方法和電腦程式產品。

【先前技術】

【0002】 在商業交易、公文簽核、證件申請、身份查核、物資發放等許多場合中，經常會使用紙張來供其中一造(以下稱爲簽章人)簽署姓名，並做爲簽章保存的載體。這樣的簽章方式不僅浪費了許多紙張，也需要額外的實體儲存空間來存放已簽署的文件，無論從環保或經濟的角度而言都是很不理想的方式。

【0003】 另外，在前述的許多場合中，簽章人(例如消費者、到銀行或政府單位洽公的人、物資請領人等)通常需要親自前往簽章請求者(例如商店店員、銀行行員、政府單位職員、物資發放人員等)所在的特定地點，辦理文件的簽章和進行其他相關的手續。在這種情況下，簽章人對於簽章請求者的身分真實性通常會有較高的信賴，但簽章請求者卻很難核實簽章人的身分真實性。因此，在許多情況下簽章請求者往往會要求簽章人提供相關的身分證明文件

來佐證其身分。若簽章人沒有隨身攜帶身分證明文件，或攜帶的證明文件不齊全，便得再跑一趟才能完成文件簽章的程序，對簽章人而言是非常不方便的事。

【0004】 要省去查驗簽章人的身分證明文件的手續，可考慮採用電子簽章的方式來核實簽章人的身分真實性。但如何核對簽章的真實性和確保資料傳輸的安全性，又能兼顧簽章請求者和簽章人雙方進行操作時的便利性，一直是電子簽章機制設計上難以突破的瓶頸。

【發明內容】

【0005】 有鑑於此，如何以能核對簽章的真實性和確保資料傳輸安全性的電子簽章機制來取代傳統的紙本簽名方式，並提升電子簽章的便利性，實爲迫切需要解決的問題。

【0006】 本說明書提供了一種雙通道電子簽章系統的實施例，其包含有：一簽章核對伺服器；一簽章請求者裝置，用於計算與一目標文件的內容對應的特徵值、對待簽章的該特徵值與一傳送目的地信息進行編碼以產生一第一圖形、並輸出該第一圖形；以及一手持裝置，用於擷取並解碼該第一圖形的影像以取得該特徵值、對該特徵值進行電子簽章以產生一簽章資料、對該簽章資料進行編碼以產生一第二圖形、並將該第二圖形傳送至一目的網址；其中若該第二圖形所包含的該簽章資料通過該簽章核對伺服器的核對程序，則該簽章核對伺服器會將與該第二圖形相對應的一核對圖形傳送至該簽章請求者裝置。

【0007】 本說明書提供了一種電腦程式產品，允許一簽章請求者裝置執行電子簽章請求運作，該電子簽章請求運作包含有：計算與一目標

文件的內容對應的特徵值；對待簽章的該特徵值與一傳送目的地信息進行編碼，以產生一第一圖形；以及利用該簽章請求者裝置的一輸出裝置輸出該第一圖形。

【0008】 本說明書提供了一種電腦程式產品，允許一手持裝置執行電子簽章運作，該電子簽章運作包含有：利用該手持裝置的一影像擷取裝置擷取一第一圖形的影像；解碼該第一圖形的影像以取得一特徵值；對該特徵值進行電子簽章以產生一簽章資料；對該簽章資料進行編碼，以產生一第二圖形；利用該手持裝置的一傳送裝置將該第二圖形或該簽章資料傳送至一目的網址；以及利用該手持裝置的一顯示裝置顯示該第二圖形。

【0009】 利用前述的雙通道電子簽章系統和相關的電腦程式產品，不僅可大幅提升文件簽章過程的無紙化程度，也無需耗費實體空間來儲存紙本文件，可同時滿足環保和經濟的目的。

【圖式簡單說明】

【0010】 圖1爲本發明的雙通道電子簽章系統的一實施例簡化後的功能方塊圖。

【0011】 圖2至圖4爲本發明之使用圖形碼的電子簽章方法的多個實施例簡化後的流程圖。

【0012】 圖5爲本發明之雙通道電子簽章系統的另一實施例簡化後的功能方塊圖。

【實施方式】

【0013】 以下將配合相關圖式來說明本發明之實施例。在這些圖式中，相同的標號表示相同或類似的元件或流程/步驟。

【0014】 在說明書及後續的請求項當中使用了某些詞彙來指稱特定的元件。所屬領域中具有通常知識者應可理解，同樣的元件可能會用不同的名詞來稱呼。本說明書及後續的請求項並不以名稱的差異來作爲區分元件的方式，而是以元件在功能上的差異來作爲區分的基準。在通篇說明書及後續的請求項當中所提及的「包含」爲一開放式的用語，故應解釋成「包含但不限定於…」。

【0015】 在此所使用的「及/或」的描述方式，包含所列舉的其中之一或多個項目的任意組合。另外，除非本說明書中有特別指明，否則任何單數格的用語都同時包含複數格的涵義。

【0016】 請參考圖1，其所繪示爲本發明一實施例的雙通道電子簽章系統(dual-channel electronic signature system)100簡化後的功能方塊圖。雙通道電子簽章系統100包含有簽章請求者裝置(signature requester device)110、手持裝置120、以及簽章核對伺服器(signature verification server)130。如圖1所示，簽章請求者裝置110包含有處理器模塊111、儲存裝置112、輸出裝置113、接收裝置114、以及儲存在儲存裝置112中的簽章請求模塊(signature requesting module)115。手持裝置120包含有處理器模塊121、儲存裝置122、顯示裝置123、傳送裝置124、簽章資料產生模塊(signature data generator module)125、影像擷取裝置126、以及儲存在儲存裝置122中的簽章啓動模塊(signature activator module)127。

【0017】 在本實施例中，簽章請求模塊115和簽章啓動模塊127都是以電腦程式實現的功能模塊。簽章資料產生模塊125則是專屬於手持裝置120的合法使用者的硬體裝置或軟體模塊，用於依據簽章啓動

模塊127的控制而執行電子簽章的動作，以產生簽章資料。例如，簽章資料產生模塊125可以是儲存有手持裝置120的合法使用者的金鑰，並貼附於手持裝置120的SIM卡上的薄型電路板(俗稱卡貼)。或者，簽章資料產生模塊125可以電腦程式實現，且儲存有手持裝置120的合法使用者的金鑰的功能模塊。

【0018】 在商業交易、公文簽核、證件申請、身份查核、物資發放等許多場合中，人們都需要親自前往某個特定地點，例如商店、銀行、政府單位、物資發放地點、主管辦公室等，與另一方的人面對面進行文件核對及簽署的動作。此時，簽章請求者(signature requester)，例如商店店員、銀行行員、政府單位職員、物資發放人員、公司部屬等，可以利用簽章請求者裝置110，將待簽署的目標文件以及簽章請求模塊115依據該目標文件的相關內容編碼產生的特殊圖形輸出給簽章人(signer)進行檢視。這裡所稱的簽章人指的是消費者、到銀行或政府單位洽公的人、物資請領人、公司主管等各種有權對特定的目標文件進行電子簽章的人。當簽章人確認目標文件的內容無誤後，可利用手持裝置120對該特殊圖形拍照，以擷取該特殊圖形的影像並解碼出其中所包含的待簽章資料。接著，手持裝置120中的簽章啓動模塊127會利用簽章資料產生模塊125對待簽章資料進行電子簽章的動作，並透過傳送裝置124將簽章後的資料傳送到簽章核對伺服器130進行簽章核對的程序。一旦簽章核對程序完成，簽章核對伺服器130便會將相關信息傳送給簽章請求者裝置110，以供簽章請求者和簽章人雙方核對。

【0019】 在應用上，簽章請求者裝置110可以是各種具運算能力、且可顯

示或列印圖形(或控制外部顯示器或印表機進行圖形的顯示或列印)的終端裝置，例如桌上型電腦、平板電腦、筆記型電腦、銷售點(point of sale，POS)裝置、收銀機裝置(cashier machine)等。手持裝置120則可以是各種具備影像擷取功能的可攜式裝置，例如行動電話、筆記型電腦、平板電腦、電子書、掌上型遊戲機等。以下將搭配圖2到圖4來進一步說明雙通道電子簽章系統100的運作方式。

【0020】 圖2爲本發明之使用圖形碼的電子簽章方法的第一實施例簡化後的流程圖。圖2的左側部分，代表處理器模塊111執行儲存裝置112中的簽章請求模塊115時，簽章請求者裝置110所進行的流程；圖2的右側部分，代表處理器模塊121執行儲存裝置122中的簽章啓動模塊127時，手持裝置120所進行的流程；而圖2的中間部分，則代表簽章核對伺服器130所進行的流程。在後續的圖3和圖4的流程圖中也都採用相同的編排邏輯。

【0021】 當簽章請求者要將一份目標文件提供給簽章人進行電子簽章時，可利用簽章請求者裝置110的處理器模塊111執行儲存裝置112中的簽章請求模塊115，以進行圖2的左側部分的流程。

【0022】 在流程202中，簽章請求模塊115會依據目標文件的至少部分內容計算該目標文件的特徵值(characteristic value)。例如，簽章請求模塊115可對目標文件的至少部分內容進行雜湊演算法的運算，並以產生的摘要(digest)信息做爲目標文件的特徵值。

【0023】 在流程204中，簽章請求模塊115會利用一預定的影像編碼演算法，將特徵值、一預設的傳送目的地信息、以及目標文件的至少部

分內容一起編碼成一圖形G1。例如，簽章請求模塊115可利用QR碼編碼演算法將前述的資料編碼成二維條碼的形式，以做爲圖形G1。實作上，傳送目的地信息可以是與簽章請求者裝置110的網路位址、裝置識別碼、或是操作者身分有關的信息。

【0024】 例如，假設簽章請求者裝置110的操作者(亦即本例中的簽章請求者)是XYZ銀行中編號爲02號的行員，則可用“XYZ-bank.com/teller#=02”或類似的字串來做爲前述的傳送目的地信息，其中“XYZ-bank.com”是XYZ銀行的網址。又例如，假設簽章請求者裝置110是ABC公司中機器編號爲TT211的設備，則可用“ABC.com/e-signature/deviceid=#TT211”或類似的字串來做爲前述的傳送目的地信息，其中“ABC.com”是ABC公司的網址。

【0025】 在流程206中，簽章請求模塊115會利用輸出裝置113將目標文件及圖形G1以顯示或列印的方式輸出給簽章人看。實作上，輸出裝置113也可以是簽章請求者裝置110用以連接外部顯示器或外部印表機的輸出埠，或者，輸出裝置113還可以包含有簽章請求者裝置110的顯示器或印表機等。

【0026】 當簽章人確認輸出裝置113所輸出的目標文件的內容無誤時，可利用手持裝置120的處理器模塊121執行儲存裝置122中的簽章啓動模塊127，以進行圖2的右側部分的流程。

【0027】 在流程208中，簽章啓動模塊127會利用影像擷取裝置126擷取輸出裝置113所輸出的圖形G1的影像。實作上，影像擷取裝置126可包含一或多個CMOS (Complementary Metal Oxide

Semiconductor）感測器、CCD（Charge Coupled Device）感測器、CMOS/CCD混合式感測器、CID（Charge Injection Device）感測器、或是其他感光元件，用來感測圖形G1的影像，並產生相對應的影像訊號。

【0028】 在流程210中，簽章啓動模塊127會利用一預定的影像解碼演算法解碼圖形G1，以從圖形G1中還原出目標文件的特徵值、預設的傳送目的地信息、以及目標文件的至少部分內容。例如，假設前述的簽章請求模塊115是利用QR碼編碼演算法來產生圖形G1，則簽章啓動模塊127可利用對應的QR碼解碼演算法來解碼圖形G1。

【0029】 在流程212中，簽章啓動模塊127會要求簽章資料產生模塊125利用所儲存的金鑰對該特徵值進行電子簽章，以產生簽章資料。

【0030】 在流程214中，簽章啓動模塊127會利用一預定的影像編碼演算法，將簽章資料以及與手持裝置120(或簽章資料產生模塊125)相對應的一硬體識別碼一起編碼成圖形G2。例如，簽章啓動模塊127可利用QR碼編碼演算法將簽章資料和前述的硬體識別碼編碼成二維條碼的形式，以做爲圖形G2。實作上，前述的硬體識別碼可以是手持裝置120的機器序號、SIM卡的號碼、簽章資料產生模塊125的裝置序號等能用來進行裝置識別的識別碼。

【0031】 在流程216中，簽章啓動模塊127會依據圖形G1所包含的傳送目的地信息決定一目的網址(destination network address)，並利用傳送裝置124將圖形G2透過第一通道傳送至該目的網址。實作上，前述的第一通道可以是網際網路中的某一特定封包傳輸路徑。在一實施例中，手持裝置120的簽章資料產生模塊125中預先儲

存有與簽章核對伺服器130的網路位址有關、且手持裝置120的使用者無法更動的一預定字串。本實施例中的簽章啓動模塊127會將該傳送目的地信息與簽章資料產生模塊125所儲存的預定字串進行組合，以產生指向簽章核對伺服器130的目的網址。例如，假設該傳送目的地信息爲字串”XYZ-bank.com/teller#=02”，且簽章核對伺服器130的經營者的網址爲”https://www.jrsys.com/”，則在簽章資料產生模塊125內儲存的預定字串，可以是例如”https://www.jrsys.com/auth/”或類似的字串。簽章啓動模塊127在流程216中可將兩字串”XYZ-bank.com/teller#=02”與”https://www.jrsys.com/auth/”組合成一目的網址”https://www.jrsys.com/auth/XYZ-bank.com/teller#=02”，並將圖形G2透過傳送裝置124傳送至該目的網址。

【0032】 如前所述，簽章啓動模塊127會藉由將圖形G1中所包含的傳送目的地信息與簽章資料產生模塊125中儲存的預定字串進行組合的方式，來決定目的網址。因此，即便簽章請求者裝置110被駭客入侵而使得僞造的傳送目的地信息被編碼在圖形G1中，簽章啓動模塊127也不可能將所產生的圖形G2傳送到簽章核對伺服器130以外的地方(例如駭客控制的釣魚網站)。如此一來，便可有效確保手持裝置120所產生的簽章資料的傳輸安全性。

【0033】 在流程218中，簽章啓動模塊127會利用顯示裝置123來顯示圖形G2。

【0034】 接著，簽章核對伺服器130會進行流程220，接收手持裝置120傳送過來的圖形G2。

【0035】 在流程222中，簽章核對伺服器130會利用一預定的影像解碼演算法解碼圖形G2，以取得圖形G2中包含的簽章資料以及與手持裝置120(或簽章資料產生模塊125)相對應的硬體識別碼。例如，假設前述的簽章啓動模塊127是利用QR碼編碼演算法來產生圖形G2，則簽章核對伺服器130可利用對應的QR碼解碼演算法來解碼圖形G2。

【0036】 在流程224中，簽章核對伺服器130會對簽章資料進行簽章核對的程序。例如，簽章核對伺服器130會在資料庫中找出與該硬體識別碼對應的金鑰，並利用該金鑰對簽章資料進行簽章核對的動作。或者，簽章核對伺服器130也可以向其他的憑證中心(certificate authority，CA)132查詢與該硬體識別碼對應的金鑰，並利用所查得的金鑰對簽章資料進行簽章核對的動作。

【0037】 若圖形G2所包含的簽章資料成功通過簽章核對伺服器130的簽章核對程序，則簽章核對伺服器130會進行流程226；否則，簽章核對伺服器130會進行流程232。

【0038】 在流程226中，簽章核對伺服器130會直接以圖形G2作爲核對圖形G2’，並透過第二通道傳送至簽章請求者裝置110。在本實施例中，前述的第二通道是指網際網路中的另一特定封包傳輸路徑，而簽章核對伺服器130可依據手持裝置120傳送圖形G2給簽章核對伺服器130時所使用的目的網址中的部分內容，取得與簽章請求者裝置110的網路位址有關的信息。例如，在前述的舉例中，手持裝置120傳送圖形G2給簽章核對伺服器130時所使用的目的網址是”https://www.jrsys.com/auth/XYZ-bank.com/teller#=02”，由於前述網址的前半部” https://www.jrsys.com/auth/”是

與簽章核對伺服器130的網址有關的預設字串，故簽章核對伺服器130會判斷前述網址的後半部”XYZ-bank.com/teller#=02”與簽章請求者裝置110的網路位址有關。

【0039】 在本實施例中，簽章核對伺服器130還會檢驗前述網址的後半部”XYZ-bank.com/teller#=02”是否屬於簽章核對伺服器130內預先儲存的有效網段(valid network segment)。若前述網址的後半部”XYZ-bank.com/teller#=02”是屬於預先儲存的有效網段，則簽章核對伺服器130會將核對圖形G2’透過網際網路傳送至簽章請求者裝置110。若前述網址的後半部”XYZ-bank.com/teller#=02”不屬於簽章核對伺服器130內預先儲存的有效網段，則簽章核對伺服器130會判定該段信息是偽造的信息。此時，簽章核對伺服器130可回傳相關的通知信息給手持裝置120。

【0040】 由前述可知，倘若簽章請求者裝置110被駭客入侵而使得偽造的傳送目的地信息被編碼在圖形G1中，導致簽章啓動模塊127將所產生的圖形G2傳送給簽章核對伺服器130時使用的目的網址的後半部中包含了偽造的傳送目的地信息，由於前述偽造的傳送目的地信息不屬於簽章核對伺服器130內預先儲存的有效網段，所以簽章核對伺服器130也不會將核對圖形G2’傳送到偽造的傳送目的地信息所對應的釣魚網站。因此，前述的電子簽章傳輸方式可有效確保手持裝置120所產生的簽章資料的傳輸安全性。

【0041】 接著，簽章請求者裝置110的簽章請求模塊115會進行流程228，利用接收裝置114接收簽章核對伺服器130傳送過來的核對圖形G2’。

【0042】 在流程230中，簽章請求模塊115會利用簽章請求者裝置110的輸出裝置113將簽章核對伺服器130傳來的核對圖形G2’以顯示或列印的方式輸出給簽章人看。此時，簽章人和簽章請求者可將輸出裝置113輸出的核對圖形G2’，與手持裝置120的顯示裝置123上所顯示的圖形G2進行核對。若輸出裝置113輸出的核對圖形G2’與顯示裝置123顯示的圖形G2兩者吻合，則簽章請求者便可確認簽章人的身分真實性，而簽章人也能確認對目標文件的簽章程序已完成，雙方無需再進行其他的身分證明文件查驗動作。

【0043】 在流程232中，簽章核對伺服器130會傳送簽章核對失敗的錯誤信息給手持裝置120。

【0044】 當手持裝置120接收到該錯誤信息時，便會將該錯誤信息顯示在顯示裝置123上，以告知簽章人。

【0045】 由前述說明可知，借助簽章核對伺服器130的簽章核對運作，簽章人只需操作隨身攜帶的手持裝置120便能完成電子簽章的程序，不需要再提供其他的身分證明文件供簽章請求者核對。這樣的方法不僅大幅簡化了整個文件簽章的流程，也同時確保簽章請求者能有效核實簽章人的身份真實性，並提升簽章人的便利性。

【0046】 圖3爲本發明之使用圖形碼的電子簽章方法的第二實施例簡化後的流程圖。圖3的方法和圖2的方法很類似，兩者的差別在於圖2中的流程216在圖3中由流程316取代、圖2中的流程220和222在圖3中由流程320取代、且圖3的方法中新增了一個流程325。前述關於圖2中的其他流程的說明，也適用於圖3的實施例。爲簡潔起見，以下僅就圖3與圖2的差異點加以說明。

【0047】 在圖3的流程316中，簽章啓動模塊127會依據圖形G1所包含的傳送目的地信息決定一目的網址，並利用傳送裝置124將在流程212中所產生的簽章資料，以及與手持裝置120（或簽章資料產生模塊125)相對應的一硬體識別碼，透過網際網路傳送至該目的網址。

【0048】 與前述圖2的方法類似，簽章啓動模塊127會藉由將圖形G1中所包含的傳送目的地信息與簽章資料產生模塊125中儲存的預定字串進行組合的方式，來決定目的網址。即便簽章請求者裝置110被駭客入侵而使得僞造的傳送目的地信息被編碼在圖形G1中，簽章啓動模塊127也不可能將所產生的簽章資料和硬體識別碼傳送到簽章核對伺服器130以外的地方(例如駭客控制的釣魚網站)。因此，前述的電子簽章傳輸方式可有效確保手持裝置120所產生的簽章資料的傳輸安全性。

【0049】 接著，簽章核對伺服器130會進行流程320，接收手持裝置120傳送過來的簽章資料和硬體識別碼。

【0050】 接下來，簽章核對伺服器130便會進行前述的流程224的運作。

【0051】 根據圖3的方法，若手持裝置120傳送過來的簽章資料成功通過簽章核對伺服器130的簽章核對程序，則簽章核對伺服器130會進行流程325；否則，簽章核對伺服器130會進行流程232。

【0052】 在流程325中，簽章核對伺服器130會利用一預定的影像編碼演算法，將手持裝置120傳送過來的簽章資料以及硬體識別碼一起編碼成與圖形G2相同的核對圖形G2’。例如，簽章核對伺服器130可利用QR碼編碼演算法將簽章資料和前述的硬體識別碼編碼成二

維條碼的形式，以做爲核對圖形G2’ 。

【0053】 在本實施例中，簽章核對伺服器130在進行流程325之前(例如在流程224之前)，還會檢驗手持裝置120傳送簽章資料給簽章核對伺服器130時所使用的目的網址的後半部，是否屬於簽章核對伺服器130內預先儲存的有效網段。若前述目的網址的後半部是屬於預先儲存的有效網段，則簽章核對伺服器130會進行流程325；否則，簽章核對伺服器130會判定目的網址的後半部是僞造的信息。此時，簽章核對伺服器130可回傳相關的通知信息給手持裝置120。

【0054】 由前述可知，倘若簽章請求者裝置110被駭客入侵而使得僞造的傳送目的地信息被編碼在圖形G1中，導致簽章啓動模塊127將所產生的簽章資料傳送給簽章核對伺服器130時使用的目的網址的後半部中包含了僞造的傳送目的地信息，由於前述僞造的傳送目的地信息不屬於簽章核對伺服器130內預先儲存的有效網段，所以簽章核對伺服器130也不會進行流程325。因此，圖3的電子簽章方法可有效確保手持裝置120所產生的簽章資料的傳輸安全性。

【0055】 圖4爲本發明之使用圖形碼的電子簽章方法的第三實施例簡化後的流程圖。圖4的方法和圖3的方法很類似，兩者的差別在於圖3中的流程325和226在圖4中由流程426取代、且圖3中的流程228在圖4中由流程428和429取代。前述關於圖2和圖3中的其他流程的說明，也適用於圖4的實施例。爲簡潔起見，以下僅就圖4與圖3的差異點加以說明。

【0056】 根據圖4的方法，若手持裝置120傳送過來的簽章資料成功通過簽章核對伺服器130的簽章核對程序，則簽章核對伺服器130會進行流程426；否則，簽章核對伺服器130會進行流程232。

【0057】 在流程426中，簽章核對伺服器130會將手持裝置120傳送過來的簽章資料以及硬體識別碼，透過網際網路傳送至簽章請求者裝置110。實作上，簽章核對伺服器130可依據手持裝置120傳送簽章資料和硬體識別碼給簽章核對伺服器130時所使用的目的網址中的部分內容，取得與簽章請求者裝置110的網路位址有關的信息。例如，假設手持裝置120傳送簽章資料以及硬體識別碼給簽章核對伺服器130時所使用的目的網址是”https://www.jrsys.com/auth/XYZ-bank.com/teller#=02”，由於前述網址的前半部”https://www.jrsys.com/auth/”是與簽章核對伺服器130的網址有關的預設字串，故簽章核對伺服器130會判斷前述網址的後半部”XYZ-bank.com/teller#=02”與簽章請求者裝置110的網路位址有關。在本實施例中，簽章核對伺服器130會將簽章資料和硬體識別碼透過網際網路傳送至網址”http://www.XYZ-bank.com/teller#=02”。

【0058】 實作上，簽章核對伺服器130在進行流程426之前(例如在流程224之前)，還可以檢驗手持裝置120傳送簽章資料給簽章核對伺服器130時所使用的目的網址的後半部，是否屬於簽章核對伺服器130內預先儲存的有效網段。若前述目的網址的後半部是屬於預先儲存的有效網段，則簽章核對伺服器130會進行流程426；否則，簽章核對伺服器130會判定目的網址的後半部是偽造的信息。此時，簽章核對伺服器130可回傳相關的通知信息給手持裝置120。

【0059】 由前述可知，倘若簽章請求者裝置110被駭客入侵而使得偽造的傳送目的地信息被編碼在圖形G1中，導致簽章啓動模塊127將所產生的簽章資料傳送給簽章核對伺服器130時使用的目的網址的後半部中包含了偽造的傳送目的地信息，由於前述偽造的傳送目的地信息不屬於簽章核對伺服器130內預先儲存的有效網段，所以簽章核對伺服器130也不會將簽章資料傳送給簽章請求者裝置110。因此，圖4的電子簽章方法同樣可有效確保手持裝置120所產生的簽章資料的傳輸安全性。

【0060】 接著，簽章請求者裝置110的簽章請求模塊115會進行流程428，利用接收裝置114接收簽章核對伺服器130傳送過來的簽章資料和硬體識別碼。

【0061】 在流程429中，簽章請求模塊115會利用一預定的影像編碼演算法，將簽章核對伺服器130傳送過來的簽章資料和硬體識別碼一起編碼成與圖形G2相同的核對圖形G2’。例如，簽章請求模塊115可利用QR碼編碼演算法將簽章資料和前述的硬體識別碼編碼成二維條碼的形式，以做爲核對圖形G2’。

【0062】 請注意，前述各流程圖中的流程順序只是舉例說明，並非侷限本發明的實際實施方式。例如，圖2中的流程216和218可以同時進行。圖3和圖4中的流程214和316可以對調或同時進行。另外，也可以將前設各流程圖中的流程232和234省略。

【0063】 在前述的說明中，手持裝置120與簽章核對伺服器130之間的資料傳輸通道，和簽章請求者裝置110與簽章核對伺服器130之間的資料傳輸通道，都是利用網際網路作爲傳輸媒介，但這只是一實施

例，而非侷限本發明的實際應用方式。例如，當雙通道電子簽章系統100應用於各種政府機構、企業組織、或任何非營利組織中的公文簽核環境時，簽章核對伺服器130可能是由組織內部的MIS部門所維護和操作。此時，手持裝置120與簽章核對伺服器130之間的資料傳輸通道，和/或簽章請求者裝置110與簽章核對伺服器130之間的資料傳輸通道，可以改用組織的內部網路(intranet)作爲傳輸媒介。

【0064】 在前述的實施例中，核對圖形G2’是與圖形G2相同的圖形。實作上，核對圖形G2’只要與圖形G2相對應即可，而不侷限於要完全相同。例如，在前述的流程226中，簽章核對伺服器130可擷取圖形G2的某些局部區域，例如，左半部、右半部、上半部、下半部、左上角或左下角的四分之一、右上角或右下角的四分之一、左上角的四分之一加右下角的四分之一等，來作爲核對圖形G2’。又例如，在前述的流程325中，簽章核對伺服器130可利用一預定的影像編碼演算法，將手持裝置120傳送過來的簽章資料以及硬體識別碼一起編碼成圖形G2，再擷取圖形G2的某些局部區域來作爲核對圖形G2’。同理，在前述的流程429中，簽章請求模塊115也可利用一預定的影像編碼演算法，將簽章核對伺服器130傳送過來的簽章資料和硬體識別碼一起編碼成圖形G2，再擷取圖形G2的某些局部區域來作爲核對圖形G2’。

【0065】 此外，在某些應用環境下，手持裝置120內的簽章啓動模塊127在前述的流程216和316中，也可以直接依據圖形G1所包含的傳送目的地信息決定一目的網址，而無需將該傳送目的地信息與其他字串結合。例如，當雙通道電子簽章系統100應用於各種政府機構

、企業組織、或任何非營利組織中的公文簽核環境時，圖形G1所包含的傳送目的地信息可以直接指向組織內部的MIS部門所維護和操作的簽章核對伺服器130。此時，簽章啓動模塊127在前述的流程216和316中，便可直接利用圖形G1中所包含的傳送目的地信息作爲目的網址。

【0066】 在前述的實施例中，簽章啓動模塊127在流程216或316中決定的目的網址，是指向簽章核對伺服器130，但這只是一實施例，而非侷限本發明的實際應用方式。例如，圖5爲本發明另一實施例的雙通道電子簽章系統500簡化後的功能方塊圖。圖5的雙通道電子簽章系統500和圖1的雙通道電子簽章系統100很類似，差別在於雙通道電子簽章系統500比雙通道電子簽章系統100多增加了一個轉發伺服器530。在雙通道電子簽章系統500中，手持裝置120的簽章啓動模塊127在流程216或316中所決定的目的網址，是指向轉發伺服器530而非簽章核對伺服器130。轉發伺服器530會將收到的圖形G2(或是簽章資料和硬體識別碼)再轉發給由另一個獨立單位所維護和操作的簽章核對伺服器130。換言之，轉發伺服器530和簽章核對伺服器130可以分別由兩個獨立的單位所控制。此外，在雙通道電子簽章系統500的架構下，轉發伺服器530可以同時支援多個簽章核對伺服器130的簽章核對運作，以達成不同單位間的分工，使簽章核對的解決方案提供業者能依據不同的客戶組織屬性提供更具彈性的系統架構。

【0067】 由前述說明可知，在前述的雙通道電子簽章系統100或500的架構下，利用圖2、圖3或圖4的電子簽章方法便能讓簽章人只需利用隨身攜帶的手持裝置120就完成電子簽章的動作，不需要再提供

其他的身分證明文件供簽章請求者核對。前述的方法不僅能確保簽章的真實性和資料傳輸的安全性，又能兼顧簽章請求者和簽章人雙方進行操作時的便利性，有利於進一步擴大電子簽章的應用範圍。

【0068】 此外，在傳統的電子簽章系統中，簽章人利用電腦、IC卡等設備對待簽署的目標文件進行電子簽章時，簽章人並不知道實際上產生的簽章資料的內容，甚至也不能確定簽章的真正次數，整個電子簽章的過程完全依賴簽章人對電子簽章程式和相關設備的信任。然而，在前揭的雙通道電子簽章系統100或500中，讓簽章人卻能以視覺方式觀察和核對手持裝置120產生的簽章相關資料(例如，前述的圖形G2)以及簽章請求模塊115輸出的核對資料(例如，前述的核對圖形G2’)，能有效減少被惡意人士盜簽的機會，大幅提升交易過程或其他行政程序中所需的身分驗證正確性。

【0069】 後續申請專利範圍中的某些電腦程式產品請求項全部以電腦程式流程爲依據，與前述的流程圖中的電腦程式流程內容對應一致。因此，這些電腦程式產品請求項，應當理解爲主要透過說明書記載的電腦程式實現前述解決方案的功能模組架構，而不應當理解爲主要通過硬體方式實現該解決方案的實體裝置。

【0070】 以上所述僅爲本發明之較佳實施例，凡依本發明請求項所做之均等變化與修飾，皆應屬本發明之涵蓋範圍。

【符號說明】

【0071】 100、500 雙通道電子簽章系統

【0072】 110 簽章請求者裝置

【0073】 111、121 處理器模塊

【0074】 112、122 儲存裝置

【0075】 113 輸出裝置

【0076】 114 接收裝置

【0077】 115 簽章請求模塊

【0078】 120 手持裝置

【0079】 123 顯示裝置

【0080】 124 傳送裝置

【0081】 125 簽章資料產生模塊

【0082】 126 影像擷取裝置

【0083】 127 簽章啓動模塊

【0084】 130 簽章核對伺服器

【0085】 132 憑證中心

【0086】 530 轉發伺服器

【發明申請專利範圍】

【第1項】 一種雙通道電子簽章系統，其包含有：

一簽章核對伺服器；

一簽章請求者裝置，用於計算與一目標文件的內容對應的特徵值、對待簽章的該特徵值與一傳送目的地信息進行編碼以產生一第一圖形、並輸出該第一圖形；以及

一手持裝置，用於擷取並解碼該第一圖形的影像以取得該特徵值、對該特徵值進行電子簽章以產生一簽章資料、對該簽章資料進行編碼以產生一第二圖形、並將該第二圖形傳送至一目的網址；

其中若該第二圖形所包含的該簽章資料通過該簽章核對伺服器的核對程序，則該簽章核對伺服器會將與該第二圖形相對應的一核對圖形傳送至該簽章請求者裝置。

【第2項】 一種電腦程式產品，允許一簽章請求者裝置執行電子簽章請求運作，該電子簽章請求運作包含有：

計算與一目標文件的內容對應的特徵值，其中該特徵值爲該目標文件的摘要(digest)信息；

對待簽章的該特徵值與一傳送目的地信息進行編碼，以產生一第一圖形；以及

利用該簽章請求者裝置的一輸出裝置輸出該第一圖形。

【第3項】 如請求項2所述的電腦程式產品，其中產生該第一圖形的流程包含有：

對待簽章的該特徵值、該傳送目的地信息、和該目標文件的至少

部分內容進行編碼，以產生該第一圖形。

【第4項】 如請求項2所述的電腦程式產品，其中輸出該第一圖形的流程包含有：

利用該簽章請求者裝置的一顯示裝置顯示該第一圖形。

【第5項】 如請求項2所述的電腦程式產品，其中該第一圖形爲二維條碼。

【第6項】 如請求項2所述的電腦程式產品，其中該電子簽章請求運作另包含有：

利用該簽章請求者裝置的一接收裝置自一簽章核對伺服器接收一核對圖形；以及

利用該輸出裝置輸出該核對圖形；

其中該核對圖形與參與一電子簽章運作的一手持裝置上所顯示的一第二圖形相對應。

【第7項】 如請求項2所述的電腦程式產品，其中該電子簽章請求運作另包含有：

利用該簽章請求者裝置的一接收裝置自一簽章核對伺服器接收一簽章資料；

對該簽章資料進行編碼，以產生一核對圖形；以及

利用該輸出裝置輸出該核對圖形；

其中該核對圖形與參與一電子簽章運作的一手持裝置上所顯示的一第二圖形相對應。

【第8項】 一種電腦程式產品，允許一手持裝置執行電子簽章運作，該電子簽章運作包含有：

利用該手持裝置的一影像擷取裝置擷取一第一圖形的影像；

解碼該第一圖形的影像以取得一特徵值；

對該特徵值進行電子簽章以產生一簽章資料；以及

利用該手持裝置的一傳送裝置將該簽章資料或依據該簽章資料編碼產生的一第二圖形傳送至一目的網址。

【第9項】 如請求項8所述的電腦程式產品，其中解碼該第一圖形的流程包含有：

解碼該第一圖形的影像以取得該特徵值、一傳送目的地信息、以及該目標文件的至少部分內容。

【第10項】 如請求項9所述的電腦程式產品，其中該電子簽章運作另包含有：

將該傳送目的地信息與一預定字串組合，以產生該目的網址。

【第11項】 如請求項10所述的電腦程式產品，其中該預定字串是儲存在該手持裝置內的一簽章資料產生模塊中，且該手持裝置的使用者無法更動。

【第12項】 如請求項8所述的電腦程式產品，其中產生該簽章資料的流程包含有：

利用該手持裝置內的一簽章資料產生模塊對該特徵值進行電子簽章以產生該簽章資料。

【第13項】 如請求項8所述的電腦程式產品，其中該第一圖形爲二維條碼。

【第14項】 如請求項8所述的電腦程式產品，其中產生該第二圖形的流程包含有：

對該簽章資料及一硬體識別碼進行編碼，以產生該第二圖形。

【第15項】 如請求項8所述的電腦程式產品，其中將該簽章資料傳送至該目的網址的流程包含有：傳送裝置將該簽章資料及一硬體識別碼傳送至該目的網址。

【發明圖式】

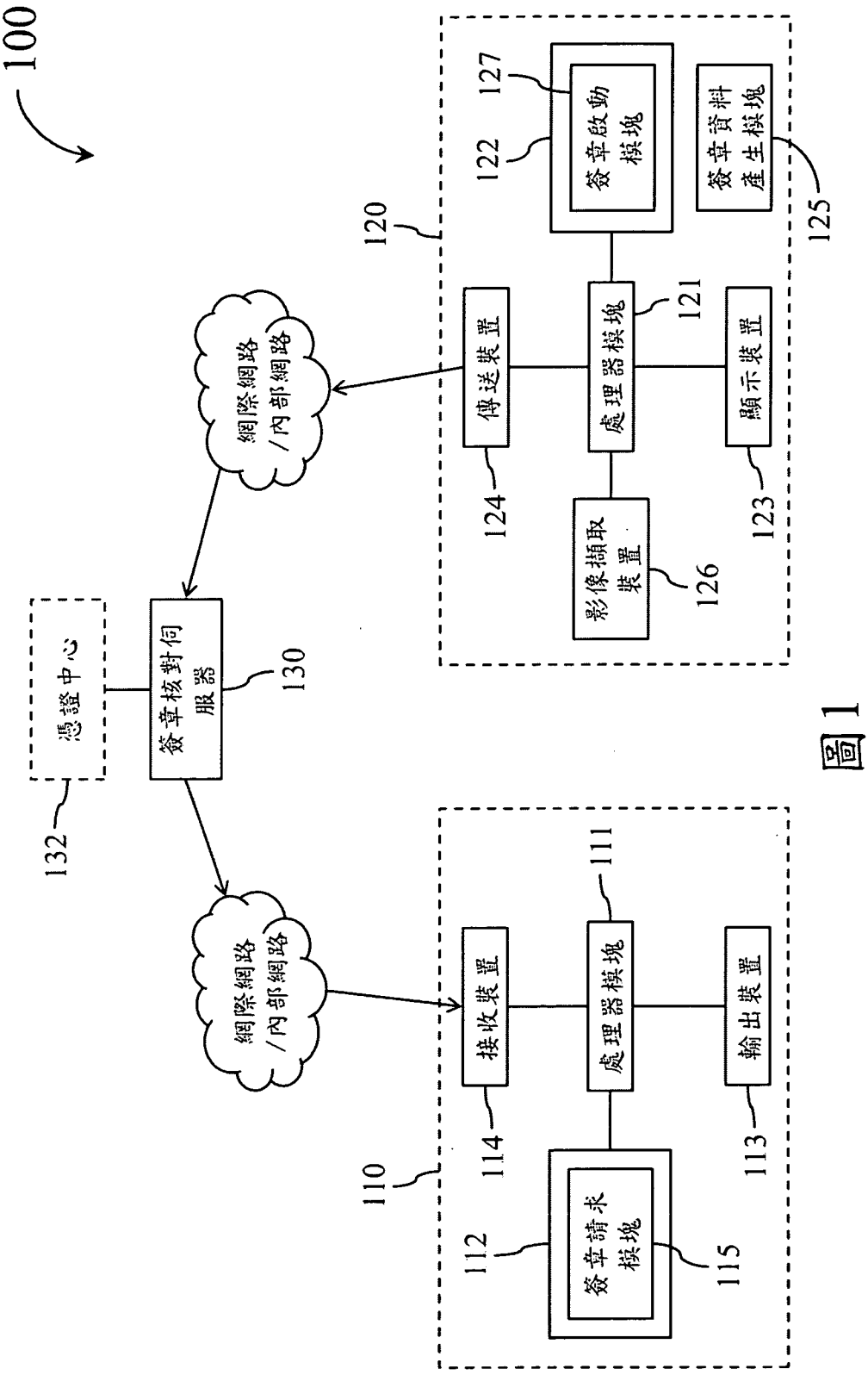
100
120
127
122
簽章啟動模塊
簽章資料產生模塊
125
傳送裝置
處理器模塊
121
顯示裝置
124
影像擷取裝置
126
123
網際網路/內部網路
憑證中心
簽章核對伺服器
130
132
網際網路/內部網路
111
接收裝置
處理器模塊
輸出裝置
110
114
113
112
簽章請求模塊
115

圖1

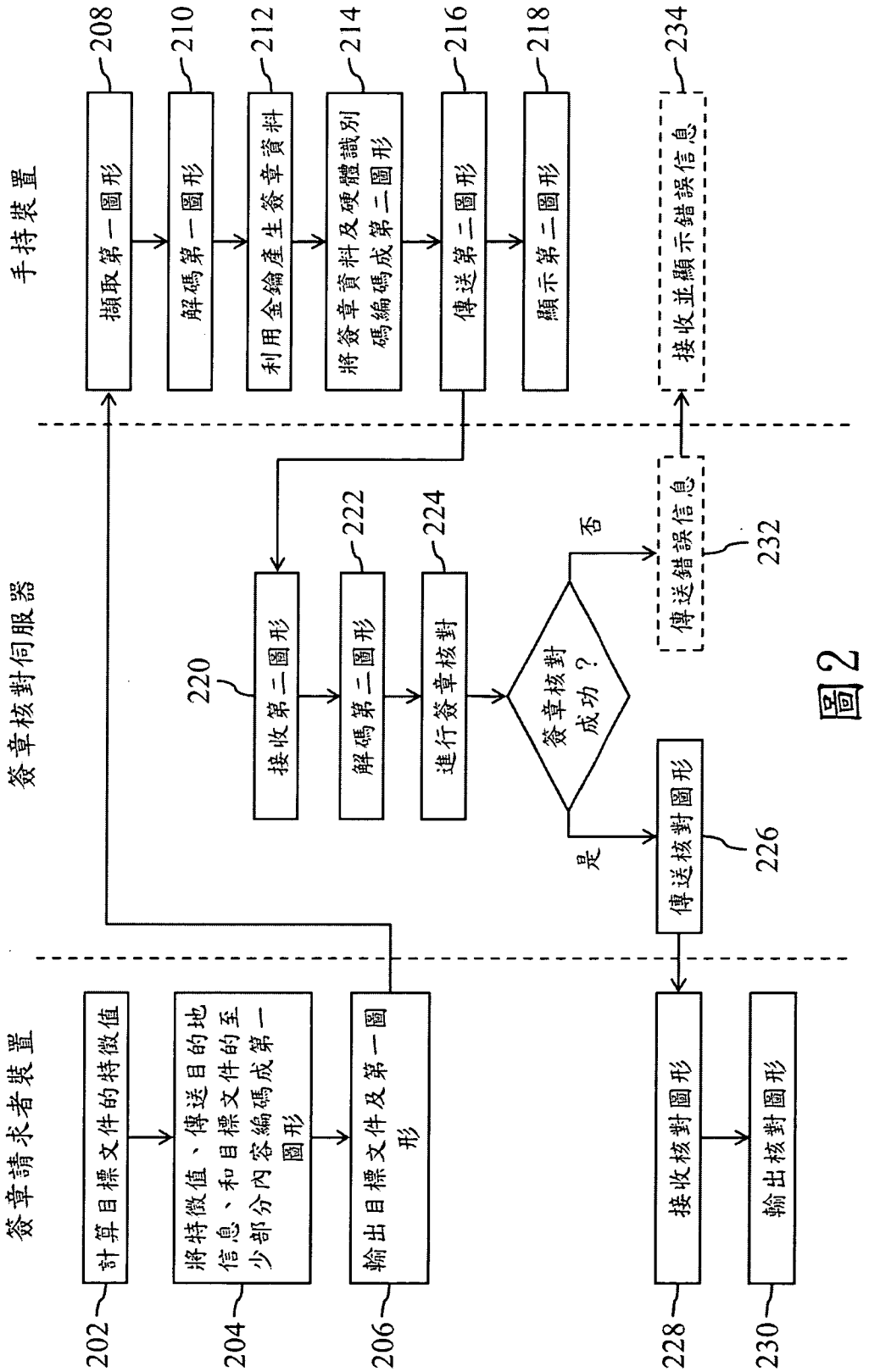
簽章請求者裝置
簽章核對伺服器
手持裝置
計算目標文件的特徵值
202
將特徵值、傳送目的地信息、和目標文件的至少部分內容編碼成第一圖形
204
輸出目標文件及第一圖形
206
接收第二圖形
220
解碼第二圖形
222
進行簽章核對
224
簽章核對成功？
否
是
傳送錯誤信息
232
傳送核對圖形
226
接收核對圖形
228
輸出核對圖形
230
擷取第一圖形
208
解碼第一圖形
210
利用金鑰產生簽章資料
212
將簽章資料及硬體識別碼編碼成第二圖形
214
傳送第二圖形
216
顯示第二圖形
218
接收並顯示錯誤信息
234

圖2

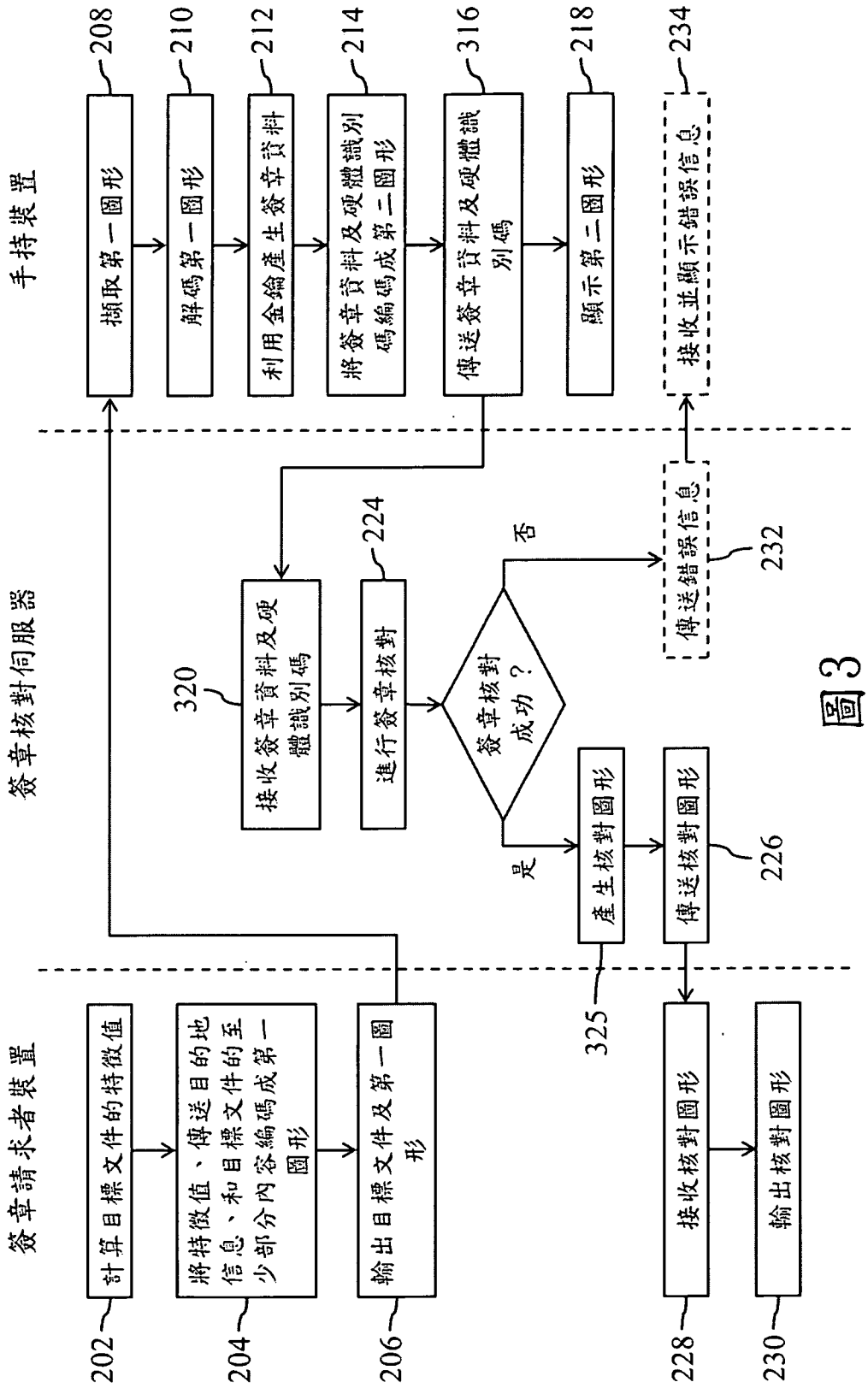
手持裝置
簽章核對伺服器
簽章請求者裝置
208
210
212
214
316
218
234
擷取第一圖形
解碼第一圖形
利用金鑰產生簽章資料
將簽章資料及硬體識別碼編碼成第二圖形
傳送簽章資料及硬體識別碼
顯示第二圖形
接收並顯示錯誤信息
320
224
232
接收簽章資料及硬體識別碼
進行簽章核對
簽章核對成功？
否
傳送錯誤信息
是
產生核對圖形
傳送核對圖形
226
325
計算目標文件的特徵值
將特徵值、傳送目的地信息、和目標文件的至少部分內容編碼成第一圖形
輸出目標文件及第一圖形
接收核對圖形
輸出核對圖形
202
204
206
228
230

圖3

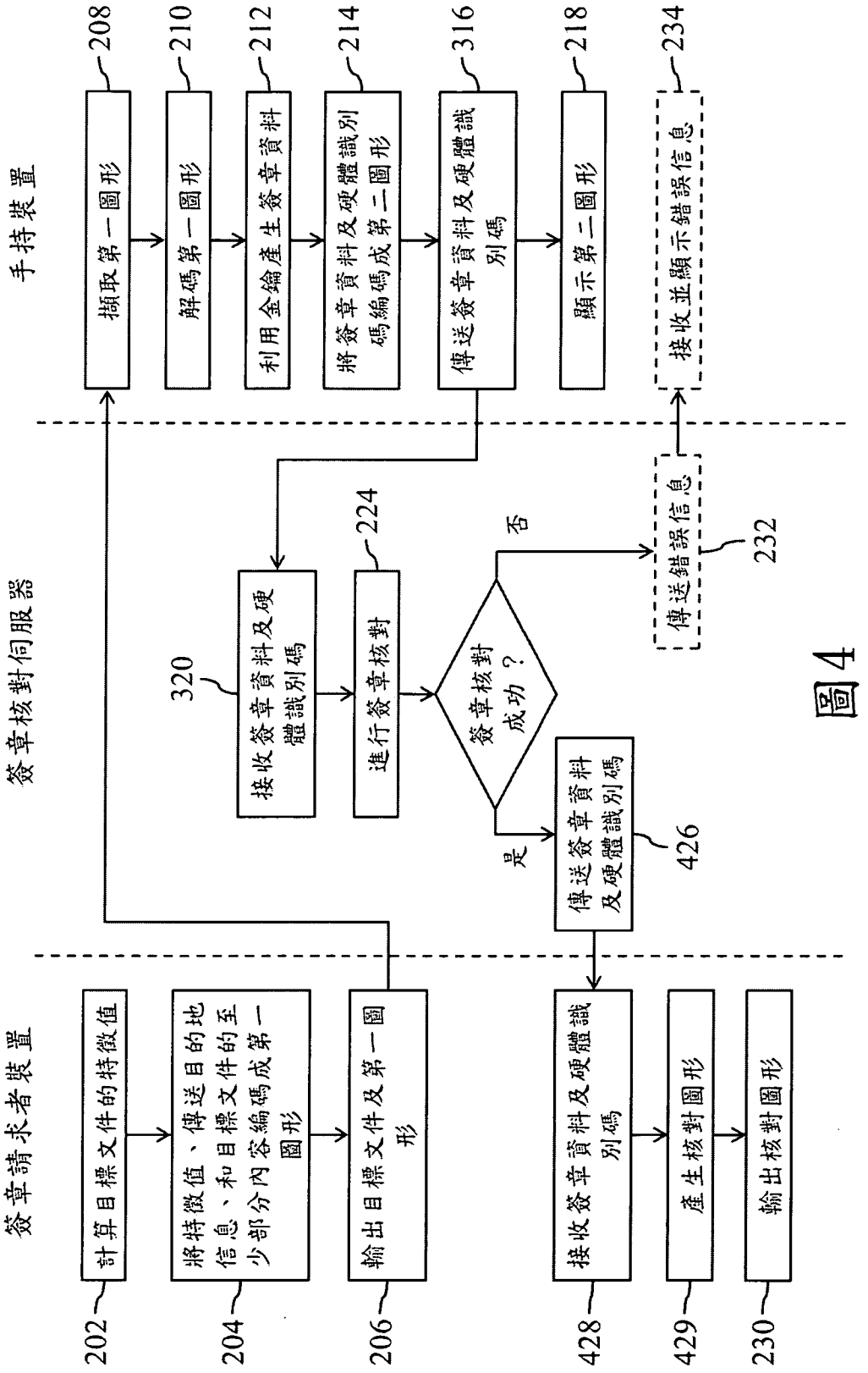
手持裝置
簽章核對伺服器
簽章請求者裝置
擷取第一圖形
208
解碼第一圖形
210
利用金鑰產生簽章資料
212
將簽章資料及硬體識別碼編碼成第二圖形
214
傳送簽章資料及硬體識別碼
316
顯示第二圖形
218
接收並顯示錯誤信息
234
傳送錯誤信息
232
否
是
簽章核對成功？
接收簽章資料及硬體識別碼
320
進行簽章核對
224
傳送簽章資料及硬體識別碼
426
計算目標文件的特徵值
202
將特徵值、傳送目的地信息、和目標文件的至少部分內容編碼成第一圖形
204
輸出目標文件及第一圖形
206
接收簽章資料及硬體識別碼
428
產生核對圖形
429
輸出核對圖形
230

圖4

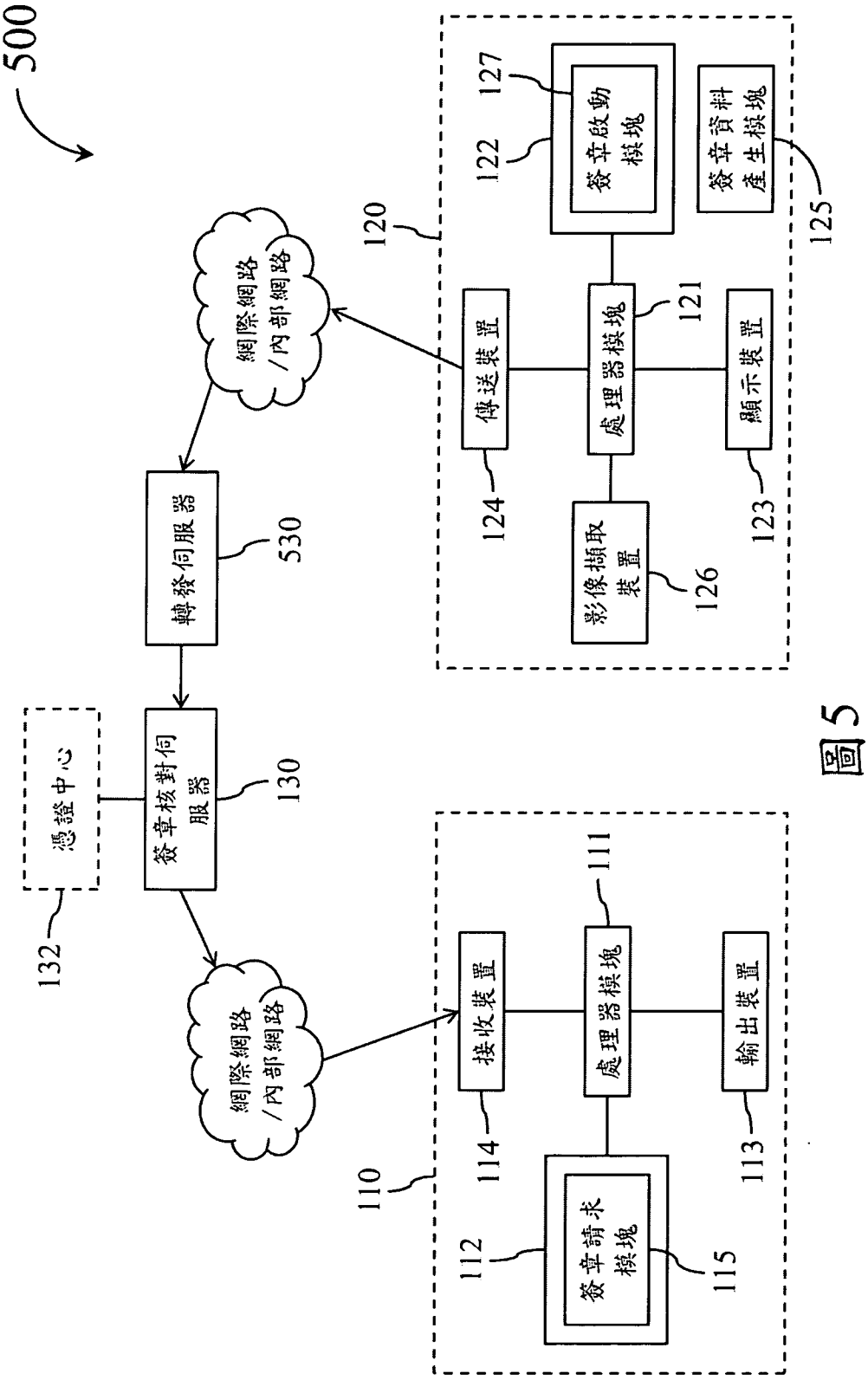
500
網際網路/內部網路
120
127
122
簽章啟動模塊
簽章資料產生模塊
125
傳送裝置
處理器模塊
121
顯示裝置
124
影像擷取裝置
126
123
轉發伺服器
530
憑證中心
簽章核對伺服器
130
132
網際網路/內部網路
111
接收裝置
處理器模塊
輸出裝置
110
114
113
112
簽章請求模塊
115

圖5