申請日期：88.4.14	案號：88105931
類別：G06F 17/60, G07F 7/08, 19/00, G07C 9/00	

（以上各欄由本局填註）

公告本

發明專利說明書

一、發明名稱	中文	數位式圖形簽章系統 525072
	英文	
二、發明人	姓名（中文）	1.克里斯 T.帕坦吉
	姓名（英文）	1.Cris T. Paltenghe
	國籍	1.美國
	住、居所	1.美國加州91326北脊市恩特拉德路11718號
三、申請人	姓名（名稱）（中文）	1.花旗集團研發中心股份有限公司
	姓名（名稱）（英文）	1.Citicorp Development Center, Inc.
	國籍	1.美國
	住、居所（事務所）	1.美國加州90066洛杉磯市西傑佛遜大道12731號
	代表人姓名（中文）	1.馬克 崔梅恩
	代表人姓名（英文）	1.

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
美國 US	1998/04/14	60/081,748	有
美國 US	1998/11/12	09/190,727	有
美國 US	1998/11/12	09/190,993	有

有關微生物已寄存於　　寄存日期　　寄存號碼

無

五、發明說明 (1)

本發明係有關於一種應用於電子交易之數位圖形簽章系統。此系統包括一文件部份及一簽章部份。文件部份具有相關於被簽署文件之相關資訊。文件及簽章部份可以進行編譯並合併為一單體而供一個人識別。「數位圖形簽章」一詞在此即代表此合併後之單體。

本發明之數位簽章系統適用於電子交易中，包括網際網路之交易。其亦可結合資訊銀行或虛擬錢包使用。

本發明亦揭露一用於私人通訊之數位圖形印記。

在實境中，簽署人可以輕易地辨認出自己的簽名。然而其真實度卻很難去確認。

相對地，在數位世界裏，數位簽名可以確保簽署人的真實性。但是，這種數位簽名卻無法以人類可以辨認的形式呈現。因此需要一個數位簽名系統，使得人們可以藉由圖像來辨認他們的簽名。除了這個問題以外，在電子交易中還有許多其他的問題有待解決。

第一個問題是關於如何向客戶提供與數位簽署文件實質內容有關之資訊。這個問題也就是「在文件以數位方式呈現時，客戶如何知道他簽署的內容是什麼？」

另一個問題則是有關於客戶與簽署文件的連結。這個問題也就是「客戶如何辨認出一份文件中的簽名是自己的？」

對於金融機構、商人、賣主或其他從事電子及非電子商務的人來說，當客戶忘記他們已簽署過的文件時，問題便會發生。這種情況可能肇因於簽名文件與賬單送達客戶

五、發明說明 (2)

間的時間過長。許多客戶會打電話要求補送有關某項交易的簽署文件。這些客戶通常都只是忘了上次的交易行為，並非惡意。在接受到交易及簽名的證明後，客戶便可以想起上次的交易，或是發現簽名做假。然而，這個過程對金融機構來說卻需要耗費大量成本在維持客服系統上，包括人員、文件處理及郵寄。

在今日的電子交易商場中，這種問題更形嚴重。現今許多技術都遇到一問題，就是在客戶簽署同意書或文件後無法得到眼見的回覆。此外，在電子交易的賬單中也無法提供足夠之資訊使客戶能記起曾進行過的交易。

本發明之系統將解決上述之問題。

本發明提供了一個系統，能夠讓個人可以辨別他們在數位文件上的簽名，並提供關於此文件之相關資訊，而使人能夠知悉簽署之內容及在以後喚起對這次簽署行為之記憶。

依據本發明，提供了一種數位圖形簽章系統，包括一圖形，經由組合簽署文件之相關細節及一個人簽章而得到。文件細節及個人簽章可以使用傳統技術進行編譯以提供保密安全。數位圖形簽章亦可以透過使用者界面而顯示出來。

被納入數位圖形簽章之文件細節包括：

簽署文件之摘要；

簽署文件之實體；

簽署文件之摘錄；或是

五、發明說明 (3)

與簽署文件相關之個人註記。

一般來說，至少包含一簽署文件所代表同意事項之摘要是被認為有需要的。這個摘要也可以包括參考資訊，例如日期、所牽涉之各方、交易編號等等。這種摘要通常以一般化(非法律字眼)之用詞撰寫，使所有客戶都能容易了解。為了形成數位圖形簽章，這個摘要通常僅包含文字。

但在某些特殊的應用中會包含圖形資料。

在某些交易中，數位圖形簽章需要將簽署文件之實體或是簽署文件的摘錄額外加入或是包含於摘要中。文件實體或摘錄通常僅包含文字，以產生數位圖形簽章。但在某些特殊應用中會包含圖形資料。

如上述，文件細節更包括一個人備忘區，讓個人可以記錄下他們自己所要記載的相關事項。一般來說，客戶會記下可以使他們以後能記憶起此次交易的事情。這種資訊可以包括交易目的、交易性質及其他重要之事項。

一個個人簽章的圖像可以包括來自一圖形或個人簽章的圖形資料。一個個人簽章圖形可以經由如圖形板(graphic tablet)等工具感應筆觸而取得簽名筆跡，亦可由掃描方式從實際文件上取得簽名。一般來說，在以下將提及的轉譯及合併動作之前，一個個人簽章圖形係與實際文件上之簽名類似。

為了產生一數位圖形簽章，文件細節資料及個人簽章資料合併在一起。合併的步驟包括使用傳統之電子編譯技術將兩組資料進行編譯。文件細節之不同部份以公眾或私

五、發明說明（4）

人鎖鑰進行編譯。

舉例來說，文件摘要資料使用簽署者之私人鎖鑰，而簽署者則使用公眾鎖鑰編碼技術簽署文件。此摘要將可以被簽署者及其他與此交易相關者讀取。

由個人輸入之備忘文字資料則可以使用一僅由簽署者知悉之對稱鎖鑰進行編譯。如此可以對簽署者提供額外的保障，確保此份文件不被偽造，並幫助他們回想交易情形。

文件細節資料及個人簽章資料可以使用如色彩編碼加以合併。在這種技術中，每一個資料流被做為如標準RGB（紅、綠、藍）色彩編譯之色彩值使用。舉例來說，摘要資料流之每一個位元可以用來產生藍色值，備忘資料流的每一個位元可以用來產生綠色值。不變紅色值可以做為描述之用。其他的色彩值也可以使用。舉例來說，CMYK色彩編碼可以使用青綠、紅、黃及黑色色彩值而產生數位圖形簽章。

數位圖形簽章可以被視為是使用「彩點」所產生一連串的墨跡，在一定義之簽名區內相對座標上的點，以及一色彩值。相對座標可以是一二維空間之x-y軸座標、r-θ軸座標，或是一三維空間之x-y-z軸座標等等。

在一開始，個人簽章資料可能包括所取得之單一色彩筆觸。在合併過程中，最初色彩值會被編譯值取代。圖點部份則可以留下以保留簽名之圖像。

簽名資料及摘要或備忘資料流之長度（位元數）的不一

五、發明說明 (5)

致可以使用一雙向填補(bidirectional padding)技術或其他熟知之技術處理。

如果簽名資料較摘要或是備忘資料長，藍色及綠色部份可以使用零值而其餘的簽名資料則使用非零值、不變之紅色色彩值。如此，即使在摘要或備忘資料結束時，簽名的圖像依然被保留。

如果簽名資料較摘要或是備忘資料短，彩點可以使用零值，而其餘的則使用色彩來編碼。訊息其餘的部份並不是簽名資料之圖像，但可能是數位圖形簽章之一部份。

此時所產生之數位圖形簽章可以維持一個與一個人簽名類似之圖像，而包括紅、綠及藍點。紅、綠及藍點之相對數量將使一數位圖形簽章及某一文件連結在一起，就如綠色及藍色點將依據文件的不同而產生。

如此技術領域之人所熟知的，不同的色彩或不同的色彩編碼方法亦可以用以產生本發明之數位圖形簽章。

數位圖形簽章可以以資料檔案之方式儲存，如.gif檔、.tiff檔、.pic檔、.jpg檔等等，並伴隨交易資料儲存。數位圖形簽章通常以可以使用一般電腦軟體(如網路瀏覽器軟體、金融交易軟體、或文書處理軟體)而藉由視訊終端顯示之檔案形式儲存。

因此，本發明之數位圖形簽章包括由複數圖點所形成之個人簽章圖像，其中該等圖點包括至少一第一組圖點，代表簽署文件資訊，以及第二組圖點，代表個人簽章。

本發明之數位圖形簽章包括一視覺可識別之個人簽章

五、發明說明（6）

的多色圖像，能夠由一視訊終端顯示，該圖像具有相對於簽署文件之唯一色彩系統。此處之視訊終端包括電腦螢幕、電視等等。

本發明之數位圖形簽章系統包括一本發明之數位圖形簽章以及能夠產生及顯示此數位圖形簽章之電腦軟硬體。該電腦硬體包括一中央處理單元、終端顯示器、記憶體、數據機、鍵盤、滑鼠、軌跡板、圖形板、掃描器、印表機或其他一般配備之電腦硬體設備。電腦硬體中最好能夠包括圖形板、電子筆、觸摸式螢幕、滑鼠、軌跡球、搖桿、或類似之輸入裝置，以取得個人簽章之筆跡。同樣或類似的輸入裝置，如鍵盤，也能夠使一個人輸入一備忘資料檔，記錄有關一簽署文件之備忘資料。

在本發明之系統中所使用之電腦軟體包括用以編譯資料流及色彩碼資料流之編譯軟體。其他的軟體，如文書處理、圖形處理等等也可能用以讓一個人輸入與交易相關之備忘資料，以及瀏覽數位圖形簽章。

本發明亦提供一種產生數位圖形簽章之方法，相對於一由個人所簽署之文件，此方法包括：

產生一該文件之摘要；

取得一該個人之簽章；

從該摘要產生一文件摘要資料流；

從該簽章產生一簽章資料流；

將該文件摘要及簽章資料流合併為一數位圖形簽章。

此方法亦更包括：

五、發明說明（7）

取得該個人之備忘資料；

產生一文件備忘資料流；

將該文件摘要、文件備忘及簽章資料流合併為一數位圖形簽章。

在另一個實施例中，本發明提供一種產生數位圖形簽章之方法，相對於一個人簽署之文件，此方法包括：

選擇與該文件有關之細節；

產生一該文件之摘要；

取得一該個人之簽章；

從該細節產生一文件細節資料流；

從該摘要產生一文件摘要資料流；

從該簽章產生一簽章資料流；

將該文件細節、文件摘要及簽章資料流合併為一數位圖形簽章。

此方法亦更包括：

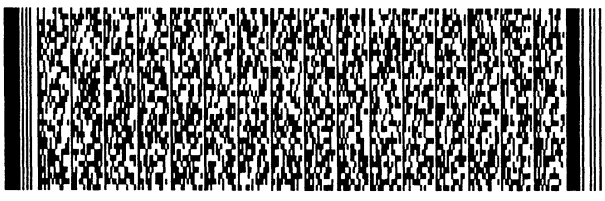
取得該個人之備忘資料；

產生一文件備忘資料流；

將該文件細節、文件摘要、文件備忘及簽章資料流合併為一數位圖形簽章。

資料流可以使用上述之方法取得以及進行合併。此外，資料流亦可被編譯。

又另一方面，本發明提供一種方法及裝置，用以提供兩方間之私人通訊，如進行交易之雙方。本發明提供一種功用，此處稱為「數位圖形印記」。數位圖形印記可以為



五、發明說明（8）

本發明之數位圖形簽章帶來額外之功用。數位圖形印記亦可單獨使用。

本發明之系統及方法較單一的數位簽章或數位認證提供了額外的功能。它們解決了客戶的需要，使客戶更安心地簽署文件，並容易地識別自己的簽名而確保他們的簽名不被偽造，也不會由其他的文件複製而來。

本發明之系統及方法亦較傳統之編譯法更人性化，使其識別度及實用性提高，例如可提供一備忘功能以幫助人們記起交易之內容。此外，本發明之數位圖形簽章亦較傳統之數位認證小，因而能更節省儲存成本及網路負載。由於它們含有一手寫簽名之圖形及數位簽名之資料，所以在數位簽章中是唯一的。

本發明之數位圖形簽章使用一類似於steganography之技術將以綠色位元值編碼之簽名備忘資料及以藍色位元值編碼之文件摘要編譯成一手寫簽名之代表圖形。

上述之技術並非一定需使用，同時也有一些訊息是以圖形來呈現及編碼的。因此，數位圖形簽章並不會隱藏雙方或多方間之通訊內容。備忘資料僅供簽名使用，並使用了只有簽署人知悉之秘密鎖鑰。任何擁有簽名之公眾鎖鑰之第三者均可確認簽名。其目的在於確認簽名之真實性以及確保交易被履行，而不是在私人間之通訊。然而必需了解的是，本發明之數位圖形簽章是可以被編譯的，且此種實施例亦落於本發明之範圍內。本發明的優點之一是不一定需要進一步之編譯。

五、發明說明 (9)

「印記」一詞係用於兩方間之私人通訊。本發明之數位圖形印記係本發明之數位圖形簽章之實施例，而更包括了兩方間之秘密通訊。數位圖形印記使用了色彩值，如使用RGB色彩系統中之紅色值來編譯及傳送一秘密通訊。以下將有詳細之說明。

藉由將一秘密通訊編成一資料流，本發明之數位圖形印記亦適用於本發明之方法。

本發明之數位圖形簽章、數位圖形印記、系統及方法適用於電子交易中，包括網際網路及網路系統之交易。本發明之數位圖形簽章系統亦可配合資訊銀行及虛擬錢包使用，如美國專利申請案號09/190,933之「Virtual Wallet System」，以及美國專利申請案號09/190,727之「Information Banking」，還有另外相關之技術，如美國專利申請案「System and Method for Securely Storing Electronic Data」、「System and Method for Controlling Transmission of Stored Information to Internet Websites」。

本發明之數位圖形簽章系統及方法之優點包括以下幾點。

人們可以藉由視覺辨認簽名。

圖形可以包括具有個人簽名之文件，但傳統之圖形卻很容易複製，因而可以輕易偽造。另外，在傳統之圖形中也沒有可以確定簽名與文件間連結之機制。相對地，本發明之數位圖形簽章不易偽造並且與簽署文件有唯一連結。

五、發明說明（10）

另一個優點是本發明之數位圖形簽章可以進行驗證。能進行驗證的人是文件之簽署人，而公眾鎖鑰係做為解開文件摘要之用。依據本發明，此摘要係被編碼成圖形簽章。此摘要必而與未被編譯前之摘要完全相合。如此顯示了文件係由客戶所簽署(因為他們是唯一擁有能夠產生簽名之私人鎖鑰的人)，且經由摘要比對，此份簽名可以連結至一簽署之文件。

另外，簽署人亦可以使用他們的私人鎖鑰讀取圖形簽章中的個人備忘資料。這種備忘資料無法由他人編入圖形簽章中，且提供簽署人額外不被偽造之保障。其亦使簽署人能夠回憶起交易之內容。

本發明之數位圖形印記之一優點為其可以包括在兩方間之秘密通訊。

本發明其他之細節及優點將配合以下之圖式做說明。

圖式簡單說明

圖1顯示本發明一實施例之數位圖形簽章；

圖2係本發明一實施例之數位圖形簽章系統之示意圖；

圖3係本發明一實施例之數位圖形簽章之流程；

圖4係本發明一實施例中簽署前之文件摘要視窗；

圖5係本發明一實施例中簽署前之文件實體視窗；

圖6係本發明一實施例中簽署前之簽名區視窗；

圖7係本發明一實施例中簽署前之簽名區發佈視窗；

圖8係本發明一實施例之簽名驗證流程；

五、發明說明（11）

圖9係本發明之數位圖形簽章系統中之簽名區預驗證之視窗；

圖10係本發明之數位圖形簽章系統中之簽名區發佈驗證之視窗；

圖11本發明之數位圖形簽章系統中之公眾簽名驗證視窗；

圖12係本發明一包含數位圖形印記之數位圖形簽章系統之示意圖；

實施例

圖1顯示本發明一實施例之數位圖形簽章「John Doe」。如圖1所示，本發明之數位圖形簽章具有一可見圖像2，類似於一個人之手寫簽名。如切圖所示，此可見圖像係由多個不同顏色之單點所形成。舉例來說，可見圖像可由綠點4、藍點8及紅點6所組成。各色點之相對數字及位置隨每一次交易而不同，並依據文件及簽名資料種類、數量之不同而以不同之色彩編碼，形成一數位圖形簽章。然而一般說來，整體之可見圖像將會與原簽署人之手寫簽名類似，以方便辨認。

一簡單的數位圖形簽章實施例包括一圖形使用者界面（GUI或UI），讓使用者可以看到：

（1）簽署文件之摘要；

（2）簽署文件之實體或細節；

（3）一簽名區，使簽署人可以以圖形方式簽名；

（4）一個人備忘區。

五、發明說明（12）

文件摘要包括客戶在簽署文件後所代表同意之事項。摘要最好使用一般化之用詞（非法律用詞），並僅以文字呈現（去除圖形）。事實上，摘要即是簽署之內容。摘要可以額外包括其他相關的事項，如日期、各方之姓名。

一旦客戶讀完文件並欲簽署時，他們會移至簽名區並以圖畫方式簽入他們的姓名。另外，客戶亦被鼓勵去輸入一些個人備忘資料以使他們能記起此次之交易。

簽名之字跡、備忘資料係由一電腦系統、及其軟硬體來完成。此外，電腦系統將會將摘要之本文及備忘資料編碼成圖形簽章。

首先，使用現代之圖形編譯法將兩個訊息流進行編譯。摘要可以使用現代公眾鎖鑰編碼技術將一客戶之私人鎖鑰編入摘要中。備忘文字則可以使用一僅由客戶知悉之對稱鎖鑰來編譯。

這兩個編譯後之訊息流便被做為標準紅、綠、藍色彩編碼中之色彩值使用。舉例來說，摘要流中之每一位元值會被做為藍色值使用，而備忘資料流中之每一位元值會被做為綠色值使用。一不變之紅色值將會做為色彩描述使用。

圖形簽章係被定義為一連串色點之墨跡，色點即是在簽名區中之x-y座標中之點及其色彩值。這些墨跡起初是以單色擷取。在編碼過程中，色彩值被編碼後之編譯文字所取代。各點之位置被保留以保存簽名之圖像。

圖形簽章筆跡、摘要及備忘資料流之位元長度之不

五、發明說明 (13)

同，藉由雙向填補技術來處理。如果圖形簽章長度大於另兩個資料流，藍色及綠色部份則使用零值，且僅使用非零、不變之紅色值。如此，簽名之圖像可以保留，即使在訊息結束時。如果兩個訊息中之一的長度大於圖形簽章，色點則被指定給零點值，而其他訊息仍然使用色彩進行編碼。這種界面並非用以取得筆跡位置，無筆跡之部份仍然保留訊息。

使用者之簽名圖像與一數位簽章合併為一個單體。這種單體具有數項優點，包括以下幾點。

客戶可以輕易地辨認出他們的簽名。圖形可以包括客戶簽名。然而，一般的圖形可以容易地被複製，也可以容易地被偽造。另外，在傳統之圖形中也無法安全地將其與一簽署文件連結。

能進行驗證的人是文件之簽署人，而公眾鎖鑰係做為解開文件摘要之用。依據本發明，此摘要係被編碼成圖形簽章。此摘要必而與未被編譯前之摘要完全相合。如此顯示了文件係由客戶所簽署(因為他們是唯一擁有能夠產生簽名之私人鎖鑰的人)，且經由摘要比對，此份簽名可以連結至一簽署之文件。

另外，簽署人亦可以使用他們的私人鎖鑰讀取圖形簽章中的個人備忘資料。這種備忘資料無法由他人編入圖形簽章中，且額外提供簽署人不被偽造之保障。其亦使簽署人能夠回憶起交易之內容。

圖2係本發明一實施例之數位圖形簽章系統之示意

五、發明說明 (14)

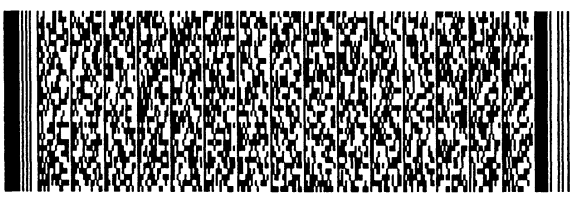
圖。如圖2所示，其包括一在非對稱編譯引擎103中使用一私人鎖鑰編譯之文件摘要102。這個過程可更包括一在對稱編譯引擎107中使用秘密對稱鎖鑰108進行編譯之秘密備忘資料106。編譯後之文件摘要及備忘資料將與一個人在簽名板上輸入之圖形簽名筆跡110一同編碼。

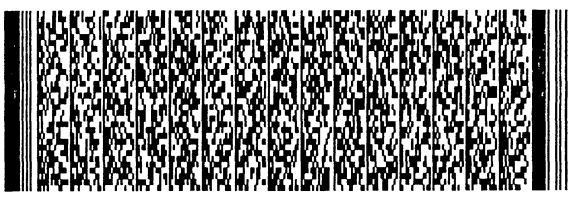
兩個編譯後之資料流被做為標準RGB色彩編碼系統中之色彩值使用。在圖2中，編譯後之摘要位元111對應於藍色，而編譯後之備忘位元113則對應於綠色。圖形簽名則使用色點112定義為一連串之墨跡。最後得到一個融合了個人簽名及數位簽章之單體114。

圖3係本發明一實施例之數位圖形簽章之流程。流程中之「訊息發送」可在一軟體中執行並回應來自使用者之輸入。如圖3所示，第一步係準備一具有摘要及實體122之數位文件。在此步驟中，文件產生軟體輸入文件之實體及一摘要至數位圖形軟體。文件由數位圖形軟體讀取，數位圖形軟體產生一文件摘要及實體126。一簡易文件摘要顯示於圖4中，而一簡易之文件實體顯示於圖5中。

如圖4所示，一文件摘要200，可以包括在一視窗204中所顯示之簽署文件相關細節202，細節202又包括標題221(摘要)、222(實體)及223(簽名)。在「摘要」之標題中，文件摘要200可以包括相關於交易行為所記載事實之細節，包括：

日期	03/23/1998
發票	352864





五、發明說明 (15)

零售商	Radioshack 01-3516
買主	Ted Smythe
信用卡	Visa
卡號	4321-2345-6789-3456
期限	04/99
交易編號	1485
授權	023598
註記	發卡銀行可調閱總金額
遵循事項	買賣及退貨依同意事項辦理
感謝	感謝您在Radio Shack購物…
應付款	27.51

圖5顯示一簡易交易之文件實體210，其摘要顯示於圖4中。如圖5所示，文件實體可包括在一視窗214中顯示之簽署文件之文字細節212，文字細節可包括標題221(摘要)、222(內容)及223(簽名)。文件實體212可以被顯示在「內容」標題下。

參閱圖3，在步驟128中，文件簽署人可以重新檢查文件摘要及內容，並輸入一些備忘資料，這些資料將在爾後幫助他們回憶起此次交易之內容。圖6顯示了一此種使用者界面可能的實施例。

如圖6所示，一簽署人界面220可以在一視窗224中執行，包括了標題221、222及223。在「簽名」之標題下，一簽署人界面220可以包括一備忘區226、一圖形簽章區228及一備忘資料輸入區230。備忘資料輸入區230可以在

五、發明說明（16）

一開始包括一文字提示，提醒使用者輸入一個人備忘資料。界面220更可以包括按鈕251（簽下）、252（確認）及253（送出），這些按鈕連結至簽名、確認及送出簽名之功能。

簽名、私人備忘資料及文件摘要被送回數位簽章132，而被編碼成使用者之簽名。圖7顯示一編碼後之圖形簽章可能的實施例140。使用者之後會被一在視窗230中之提示文字提醒送出此編碼後之圖形簽章至文件起草人以簽下此份文件，並完成其間之交易。如圖3所示，在步驟134中，被簽署後之文件及數位圖形簽章選擇性地被送至數位文件檔或一公證人以確認此數位簽章。公證人使用簽署人之公眾鎖鑰確認此簽名並非偽造。

本發明之數位圖形簽章可適用於一虛擬錢包系統。在一虛擬錢包系統中，錢包持有人之簽名會依附在發票或收據上，而可被錢包持人辨識。本發明簽署文件之最後格式由於可被人眼辨認，所以不止是一般的數位簽名。最後簽署文件之格式使持有人可以用肉眼辨認他們自己的簽名，此種格式亦將簽名及簽署文件連結在一起，且可以確認簽名或簽署之文件不被偽造。這種簽章包括一本發明之數位圖形簽章並包括數位簽名及圖形。在電子交易中，提供可辨認及區別之數位簽章之功能是前所未見的，且與簽署人在紙上作對之方式類似。這種優點使錢包持有者記起每一筆交易並可確認他們的簽名。

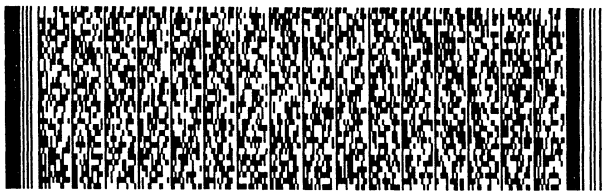
僅管使用這種格式，還是建議簽署文件能夠包括至少

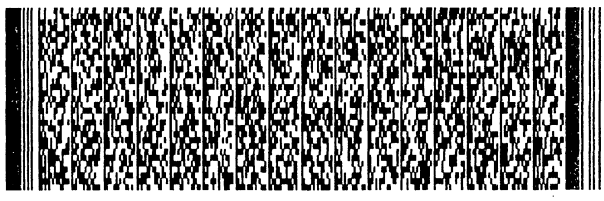
五、發明說明（17）

一摘要及實體。摘要包括客戶簽名所代表之同意事項，以一般化之用詞呈現，不含圖形之文字。摘要可以是關於付款、送貨或交易之遵循事項等等。舉例來說，摘要中之付款資料可以包括日期、交易各方、交易之性質及付款數目。實體則包括與此文件所有相關之完整資料。因此，實體包括所有與交易有關之細節。一旦文件被簽署後，它最少有三個部份：摘要、實體及簽名。然而還是可以有其他的部份，如遵循事項、貨運資料等等。所以，藉由將這種格式化之資訊送至一適用之瀏覽器就可以向買主開立發票。

在實際操作上，請參閱圖3，簽名要求人，如一家餐廳，要求買方簽署文件，如收據。簽名要求人開始整個流程並送出一文件及摘要。本發明之一特徵在於特別地將此文件及摘要格式化並將其設計為一可供軟體識別之簽名文件。當簽名文件上線時，電子錢包伺服器將此簽名文件送至一電子錢包界面，藉此，同時支援同步及非同步之對話。電子錢包界面將簽名文件及摘要顯示給買方以供簽名。買方則選取其簽名關鍵匿名並以圖形方式簽署文件。

晶片裝置使用一私人鎖鑰將此摘要進行編譯，亦使用一秘密鎖鑰將備忘資料編譯。如此使任何擁有與私人鎖鑰相配之公眾鎖鑰者可以讀取此份文件，而同時使備忘資料對買方及私人鎖鑰擁有者以外的人保密。簽署後之文件此時便包括了摘要及數位圖形簽章。藉由使用一私人鎖鑰將摘要編譯，數位圖形簽章包含了一數位簽章。





五、發明說明 (18)

再者，晶片裝置將簽署後之文件及其編號送回電子錢包伺服器。晶片裝置負責記憶此編號以使買方不用擔心。買方甚至可以處於下線狀態。電子錢包伺服器將此簽署文件存檔並送出其編號、識別符號及簽名驗證人之網址給簽名要求人，簽名要求人再將這些資料儲存。最後，簽名要求人確認收到資料。如此，本發明之優點即在於同時對多個簽名鎖鑰及其編號做管理。

當一文件已被一選定之數位圖形簽章簽暑後，此數位圖形簽章物便可在被要求時知道如何產生一簽章圖形。數位圖形簽章亦包含數位簽章。數位圖形簽章包含了第三者對簽名的認證及文件簽署者對其簽名及簽名與文件連結的確認。再者，數位圖形簽章適用於對文件真實性之確認及授權，不需繁複的數位認證。

圖8係本發明一實施例之簽名驗證流程。此流程係一已簽署文件者不確定是否已簽署一文件時，或是忘記了交易內容而需檢視備忘資料時所做之確認動作。在取得一文件後，簽署人將可檢視文件上之簽名。圖9在界面220中顯示了一可能的實施例。使用者將會在圖9之視窗230中被提醒去要求簽名驗證。在要求驗證後，隱藏之私人鎖鑰152被用來解開伴隨著簽名153之備忘資料。為了使用私人鎖鑰，使用者將會被要求輸入一密碼。隱藏之公眾鎖鑰154被用來解開簽名及文件摘要155。被解開後之備忘資料及文件摘要便與真正之備忘資料及文件摘要157進行比對，如果他們相配，則會顯示於視窗228及230中，使簽署者確

五、發明說明 (19)

認他簽過此份文件159。圖10顯示了一可能的實施例。

如圖10所示，一簽名140(Ted Smythe)被顯示於視窗228中，一個人備忘資料顯示於視窗226中及一文件摘要顯示於視窗230中。在圖10中，文件摘要對應於圖4中之摘要。

如果備忘資料、摘要及簽名無法解開，或是與文件不符，使用者會收到一警告訊息，使用者便可通知文件發送者此份文件是偽造的161。

本發明的另一特徵，請參閱圖8，更進一步地解決了客戶對識別他們自己簽名的需求。當買方需要確認他們簽名的真假時，便可以使用自己的簽名確認系統。此外，這個系統也可以在每一次文件開啟時自動地確認簽名，而只在有不符時警告買方。舉例來說，警告訊息可以是「此簽名與摘要不符」。

在此實施例中，買方從文件檔案中取得一文件及摘要，此文件檔案可以被儲存於買方之個人電腦、電子錢包伺服器或其他的裝置中。如上述，文件通常是使用數位圖形簽章簽署的。買方要求確認簽名的真假。電子錢包界面送出一公眾鎖鑰要求至保密晶片裝置，再取得此鎖鑰。此界面使用此鎖鑰解開簽名的數位部份，包括摘要。界面將解開後之摘要資訊做比對。這個比對動作便顯示了買方簽名的真假，因為他們是唯一擁有私人鎖鑰的人，且簽名僅與某份文件連結。再者，簽名的圖形部份由買方確認。如果解開後之摘要與未解開前之摘要相符，則可證明此簽名

五、發明說明（20）

之真實性。因此，電子錢包界面送回一訊息給買方，告知確認之結果。

數位及圖形比對確認之組合使得與某一文件連結之簽名得以進行驗證。這個優點是唯一的且較數位簽名來得安全。因此，這項優點證實了數位圖形簽章為原來之簽章，而非只是一個像原始簽章之簽章。

另外，這項特徵亦使得只有買方可以解開備忘資料，此資料不存於文件中，且可以提醒買方記起交易內容。

圖11係本發明之數位圖形簽章系統中之公眾簽名驗證視窗。其間之對話是在除了簽署人以外之人，如賣方或公證人，欲確認簽名時所使用。如上述，只有簽署人能夠看到備忘資料。再者，雖然選擇性的文件與數位圖形簽章比對動作並沒有顯示在圖11中，還是可以經由類似之步驟加入。

如圖11所示，當數位圖形簽章確認之要求由一第三者提出時171，簽署人的公眾鎖鑰154被用來解開文件。此公眾鎖鑰可以事先提供給要求人。公眾鎖鑰解開文件摘要173。解開之文件摘要與真正之文件摘要做比對175，且其結果或是警告訊息會顯示給要求人177。

請參閱圖11，本發明提供了一個可以經由電子郵件、直接登入或是網際網路進行電子簽章認證之服務。在此實施例中，確認要求人送出簽署後之文件、文件識別及簽署人之編號至簽名保證人。舉例來說，在網際網路上它可以是：

五、發明說明 (21)

http://www.citibank.com/verifysignature

Signature:(輸入數位圖形簽章)

of Signer:(輸入編號)

Against:(輸入文件識別)

With:(輸入摘要)

簽署人之編號是唯一對應於每一個簽名保證人，所以他們知道誰是簽署人及所使用之公眾鎖鑰。另外，文件識別可以在電子錢包伺服器中找到，在文件簽署後至少儲存了文件之摘要。最後，摘要即是確認要求人所要求要進行簽名確認之文件。

簽名保證人使用編號在公眾鎖鑰檔案中查詢公眾鎖鑰。簽名保證人使用公眾鎖鑰解開欲確認之簽名。如果簽名被解開，就表示簽名是由記載中之簽署人所簽。藉由使用文件識別，簽名保證人查詢摘要之複本，並與送出之摘要進行比對而進一步確認簽名及與簽名連結之文件的正確性。之後，簽名保證人便將確認結果送回要求人。

本發明之特徵在使用了編號及文件識別以驗證簽名。

然而，現有之方法需要包括大量資料之認證動作，如公眾鎖鑰、證書及摘要之保證人。再者，由於其需要大量之資訊，使用現有方法之簽名保證人無法確保流程之進行。而在本發明中，簽名保證人扮演一非常主動之角色。

因此，本發明之此特徵使簽名之確認更經濟也更有效率。

如以下所述，本發明之數位圖形簽章系統具有許多優

五、發明說明（22）

點。

依據本發明，數位簽章及一保密備忘資料可以被編碼為單一圖形簽章。

另一優點是圖形簽章可以由文件簽署人辨認，且文件簽署人也可以確信簽名之真實性及其與文件之連結。

再一優點是簽名的數位部份可以由一第三者進行確認，此第三者擁有此簽署人秘密鎖鑰之公眾部份。

又再一優點是與文件連結之備忘資料依然對非簽署人保密。

如本發明所述之虛擬錢包系統，-數位圖形簽章系統可以使用在一虛擬錢包系統中。

圖12係本發明一包含數位圖形印記之數位圖形簽章系統之示意圖。編譯之摘要位元111及編譯之備忘資料位元113以上述之方法產生，也由圖2所顯示。A代表進入編碼流程之資料流。同樣的，秘密備忘資料也如上述方法產生。M代表進入編碼流程之資料流。

本發明之數位圖形印記之實施例顯示於圖12，紅色位元值302被用做私人通訊。如圖12所示，一私人通訊304可以減少為文字型式並使用發送者(簽署人)之私人鎖鑰306。編譯之結果308，再使用接收者之公眾鎖鑰310進行編譯。最後之結果將被用做色點流中之紅色色彩值。

在收到通訊之後，接收者將首先使用他們的私人鎖鑰解開第一層。由於他們會接收一伴隨文件之數位圖形印記(與數位圖形簽章不同)，他們將會得知在紅色色彩值中有

五、發明說明（23）

一私人通訊，並以與數位圖形簽章不同之方式處理。一旦他們解開了第一層，便會使用發送者之公眾鎖鑰解開最後層。雙層編譯及編譯及解譯之順序之使用是有好處的。

在使用單層編譯的情況下，如果發送者使用接收者的公眾鎖鑰，就只有接收者可以解開訊息，這是我們需要的特徵。然而，如果沒有另一個數位簽章，則接收者將無法得知是否所宣稱之發送者即是真正的發送者。

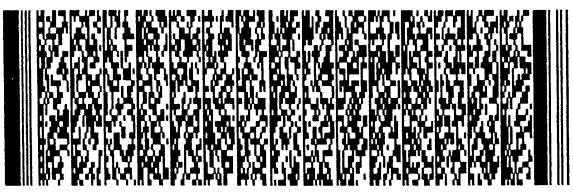
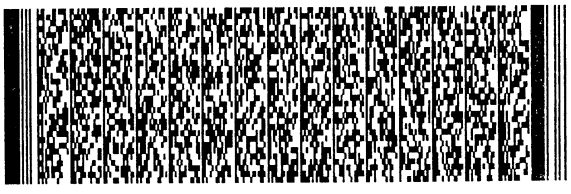
假如不使用接收者之公眾鎖鑰，而使用發送者自己的鎖鑰，接收者就可以使用發送者的公眾鎖鑰解開訊息，並將會得知只有他們送出訊息，這是另一個優點。然而這也造成了一個問題，就是任何一個知道發送者公眾鎖鑰的人也可以解開此訊息。

本發明對雙層編譯之使用是新穎且唯一的。數位化圖形印記可以是一文件之單元，所以其使用是具彈性的。

舉例來說，如果私人通訊很短，通訊的內容可以完全包含在數位圖形印記中。文件摘要可以用來傳達一般訊息，但不是細節。文件之實體可以是空的或是摘要的複本。

在較長的私人通訊中，一對稱鎖鑰會被編入數位圖形印記中，以用以解開文件實體。這並非在傳統編譯圖形學中之「session key」。數位圖形印記具有彈性之另一優點是它可以同步或非同步之方式使用。

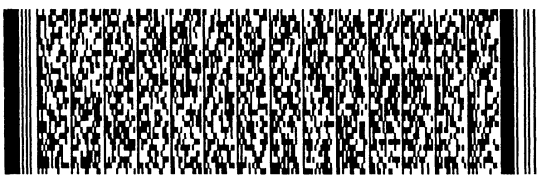
雖然數位圖形印記可以使用於所有的交易中，它利於使用於通訊中，而非進行實際線上鎖鑰之通訊。數位圖形

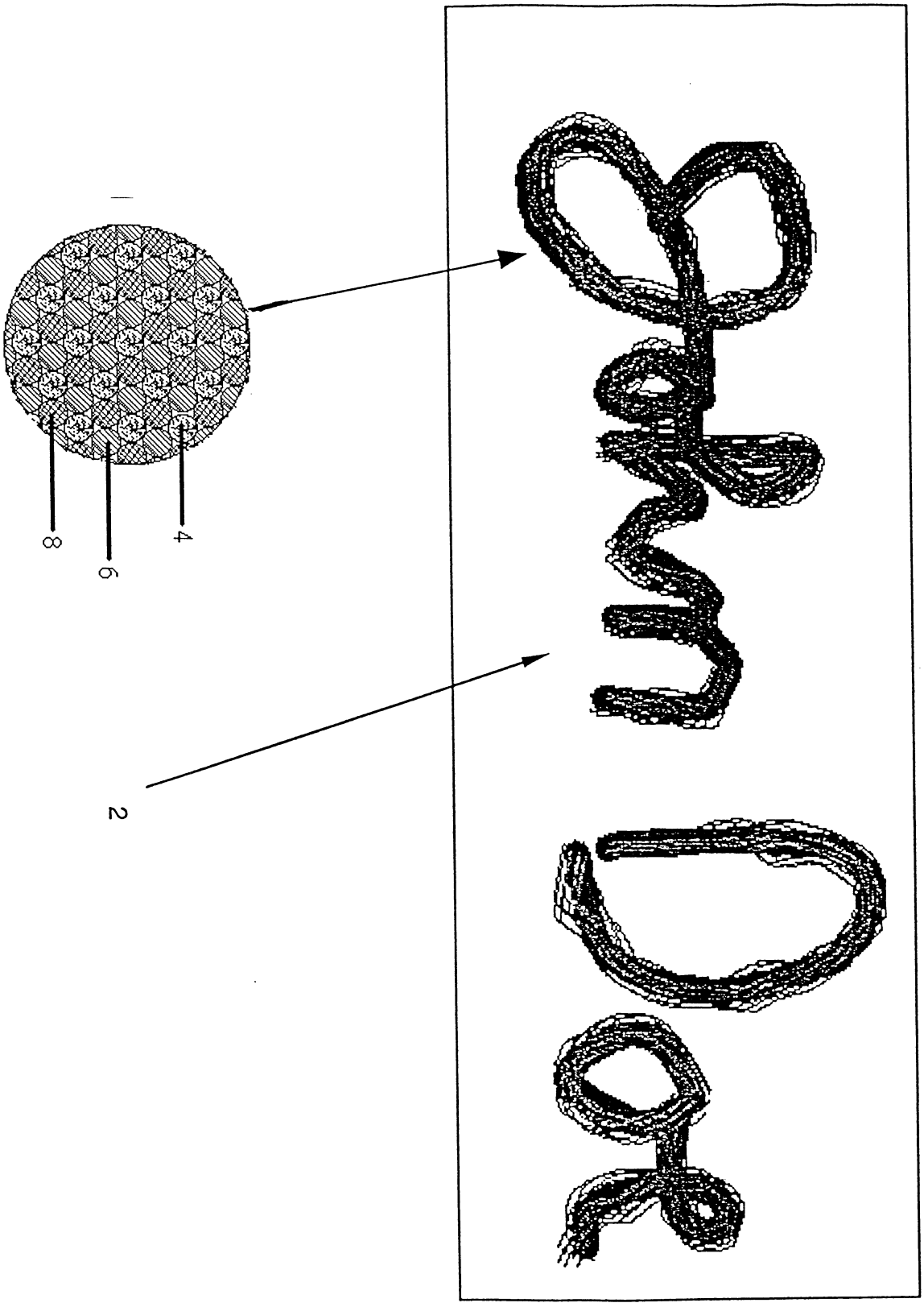



四、中文發明摘要　（發明之名稱：數位式圖形簽章系統）

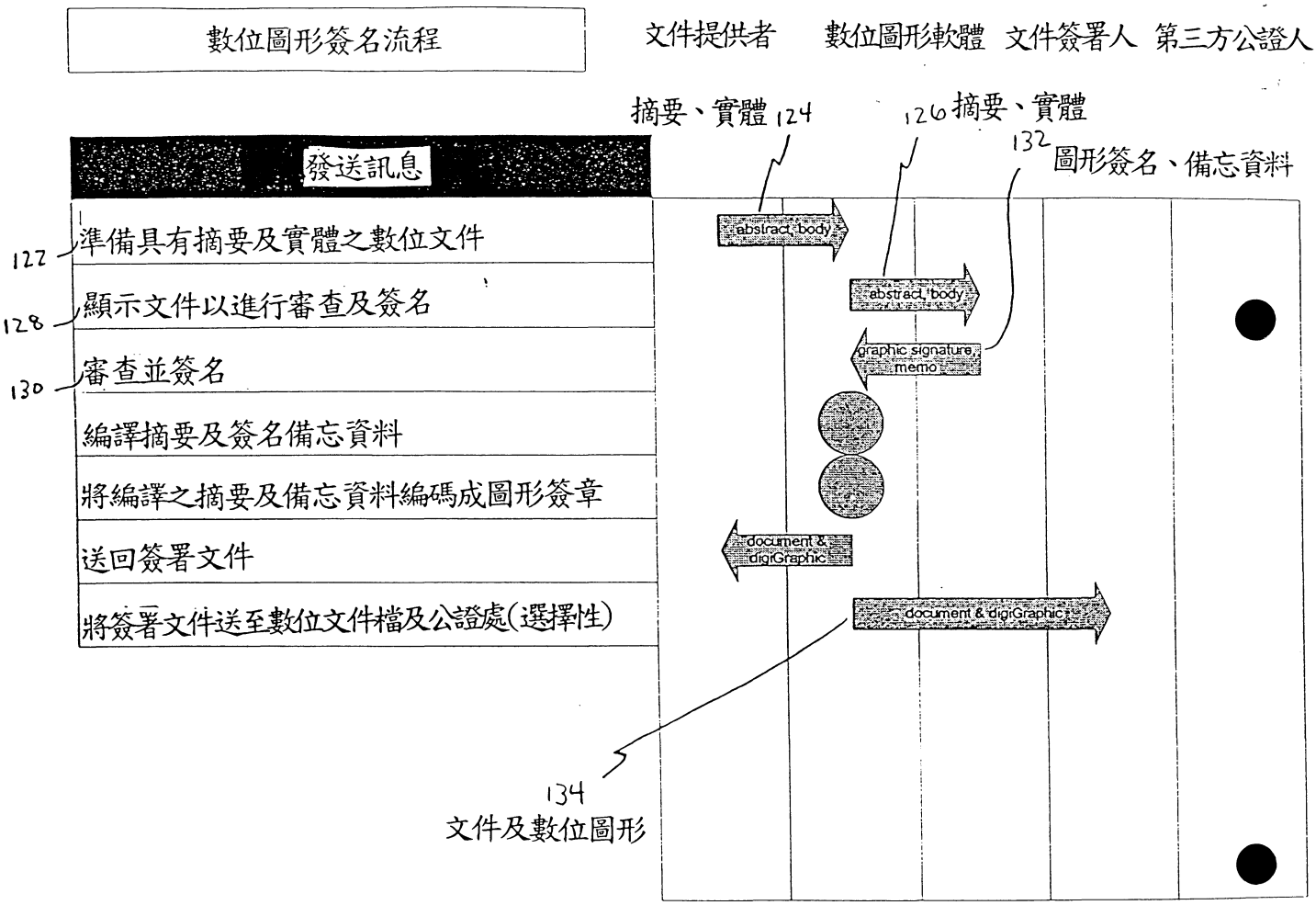
本發明提供一種應用於電子交易之數位圖形簽章系統及方法。此系統包括一文件部份及一簽章部份。文件部份具有相關於被簽署文件之相關資訊。文件及簽章部份可以進行編譯並合併為一單體而供一個人識別。「數位圖形簽章」一詞在此即代表此合併後之單體。本發明之數位簽章系統適用於電子交易中，包括網際網路之交易。其亦可結合資訊銀行或虛擬錢包使用。本發明亦揭露一用於私人通訊之數位圖形印記。

英文發明摘要　（發明之名稱：）

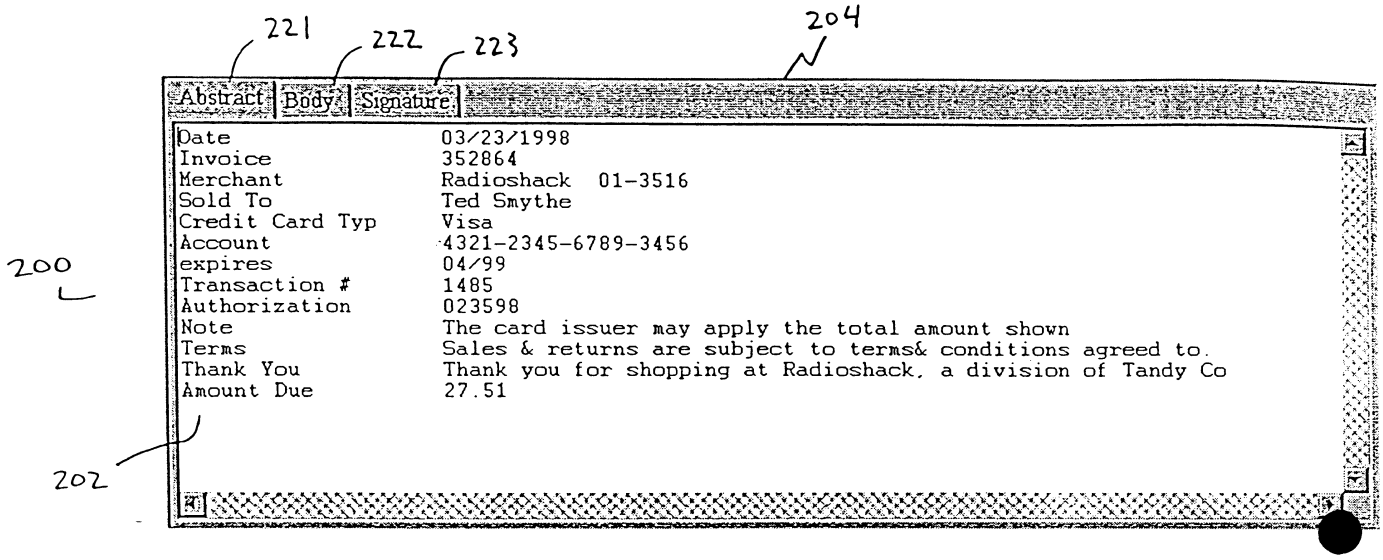




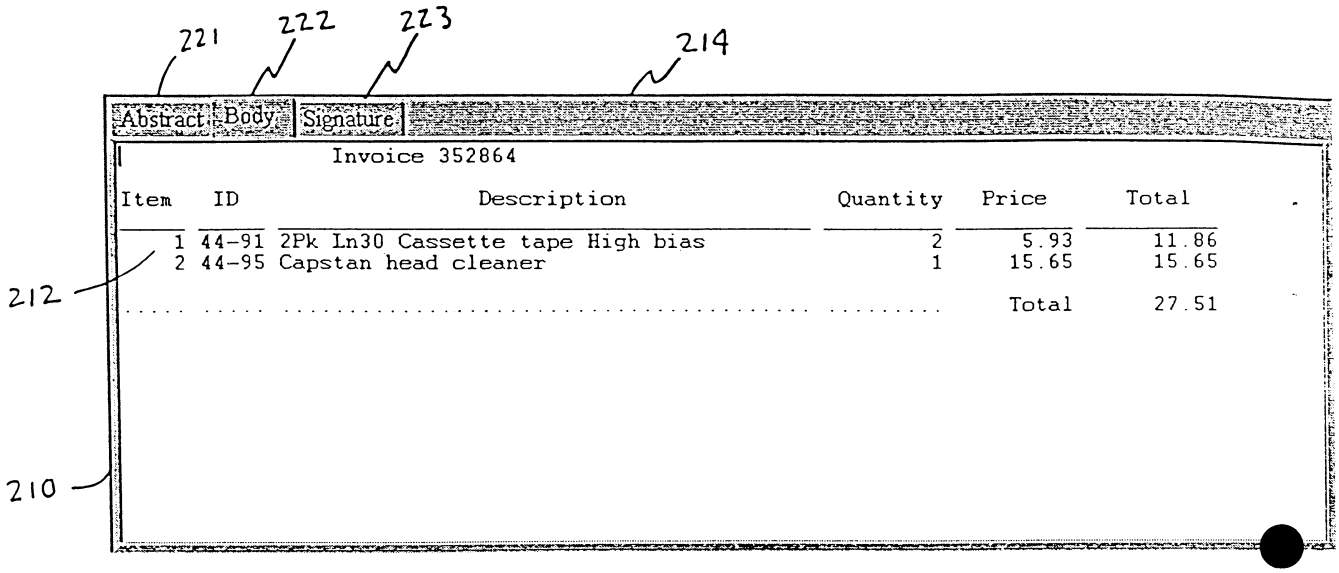
第 1 圖


數位圖形簽名流程
文件提供者
數位圖形軟體
文件簽署人
第三方公證人
發送訊息
準備具有摘要及實體之數位文件
顯示文件以進行審查及簽名
審查並簽名
編譯摘要及簽名備忘資料
將編譯之摘要及備忘資料編碼成圖形簽章
送回簽署文件
將簽署文件送至數位文件檔及公證處(選擇性)
127
128
130
摘要、實體 124
126 摘要、實體
132 圖形簽名、備忘資料
abstract, body
abstract, body
graphic signature, memo
document & digiGraphic
document & digiGraphic
134
文件及數位圖形

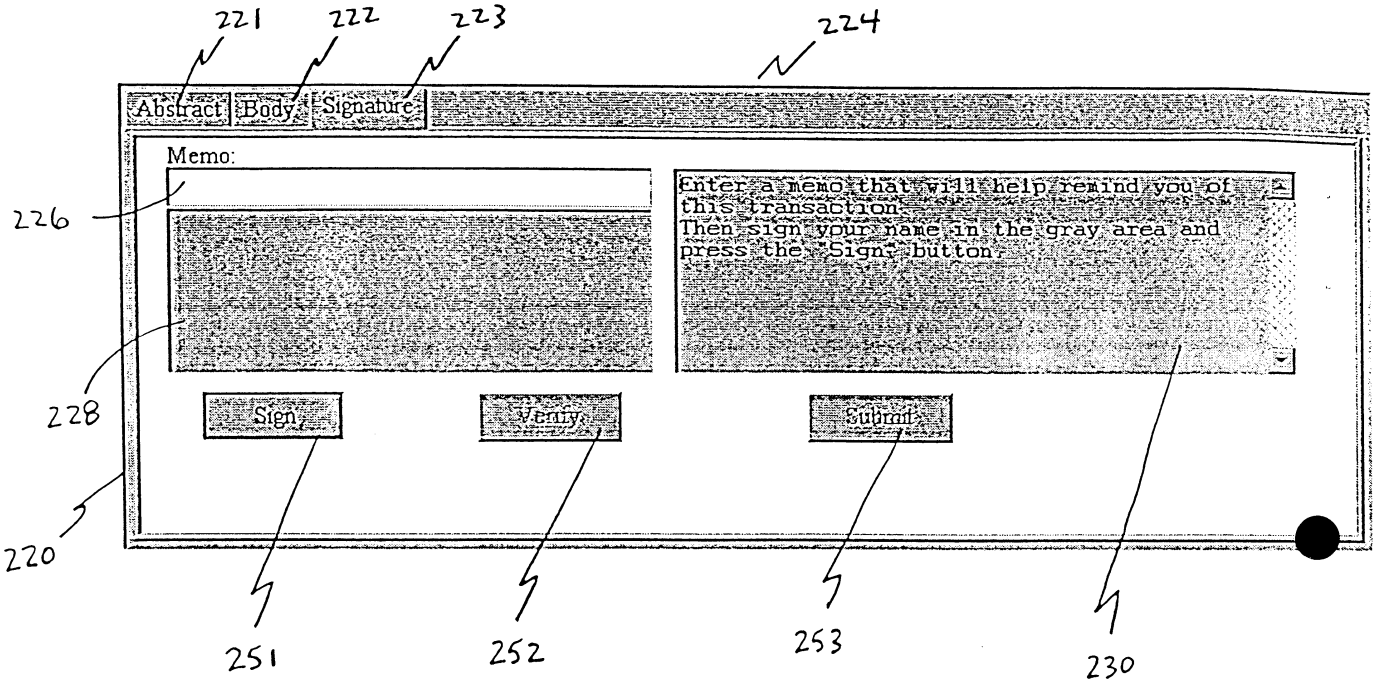
第 3 圖


221
222
223
204
Abstract
Body
Signature
Date 03/23/1998
Invoice 352864
Merchant Radioshack 01-3516
Sold To Ted Smythe
Credit Card Typ Visa
Account 4321-2345-6789-3456
expires 04/99
Transaction # 1485
Authorization 023598
Note The card issuer may apply the total amount shown
Terms Sales & returns are subject to terms& conditions agreed to.
Thank You Thank you for shopping at Radioshack, a division of Tandy Co
Amount Due 27.51
200
202

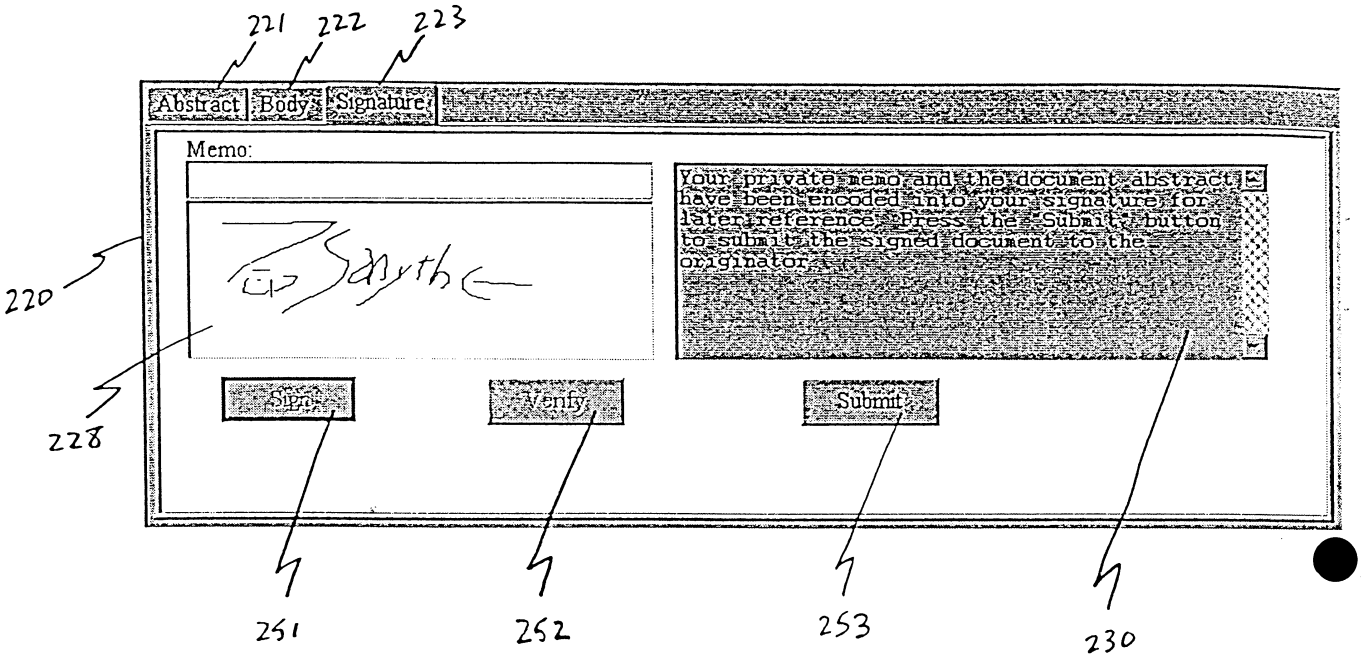
第 4 圖


221
222
223
214
Abstract
Body
Signature
Invoice 352864
Item ID Description Quantity Price Total
1 44-91 2Pk Ln30 Cassette tape High bias 2 5.93 11.86
2 44-95 Capstan head cleaner 1 15.65 15.65
Total 27.51
212
210

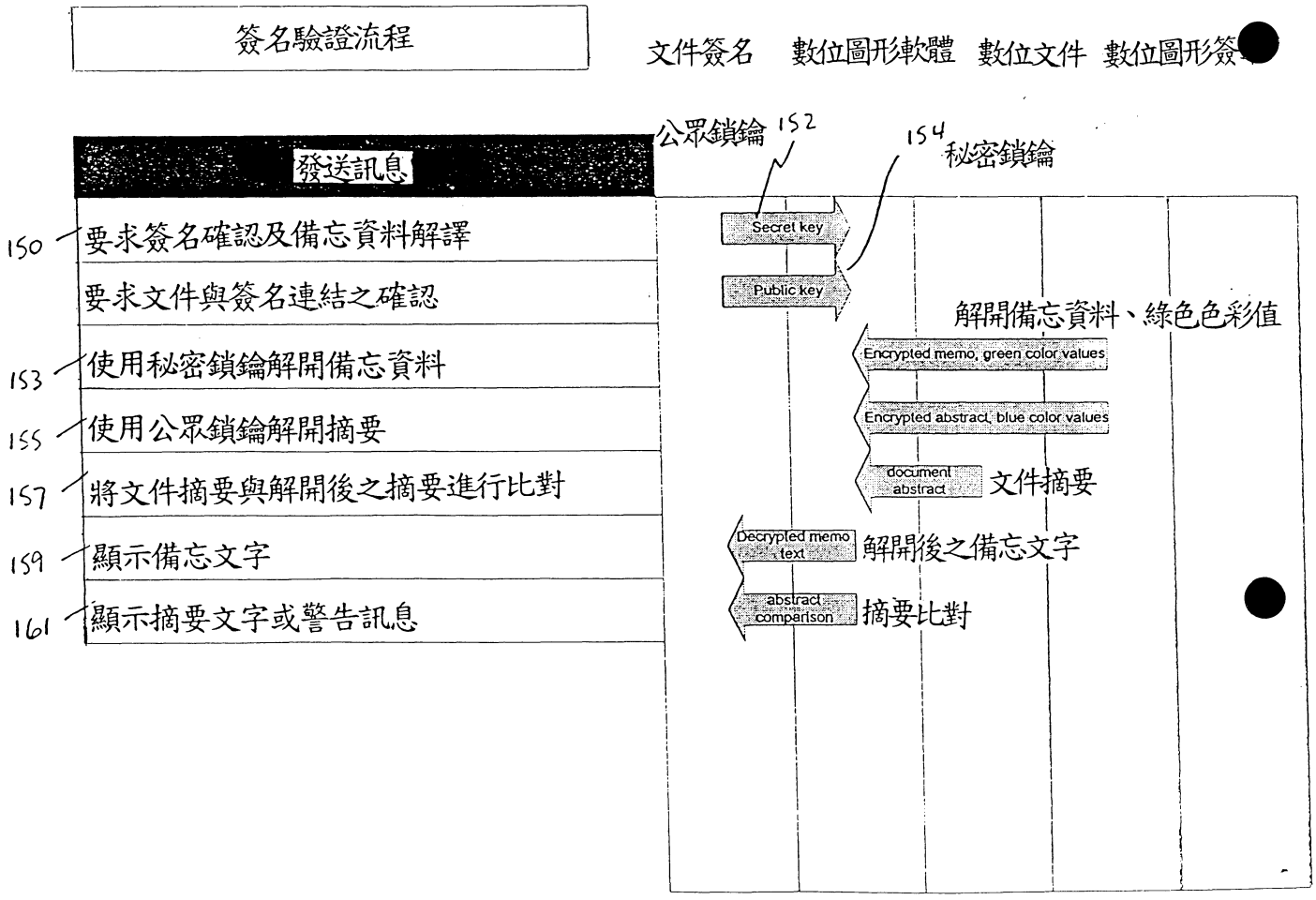
第 5 圖


221
222
223
224
Abstract
Body
Signature
Memo:
Enter a memo that will help remind you of this transaction. Then sign your name in the gray area and press the "Sign" button.
226
228
Sign
Verify
Submit
220
251
252
253
230

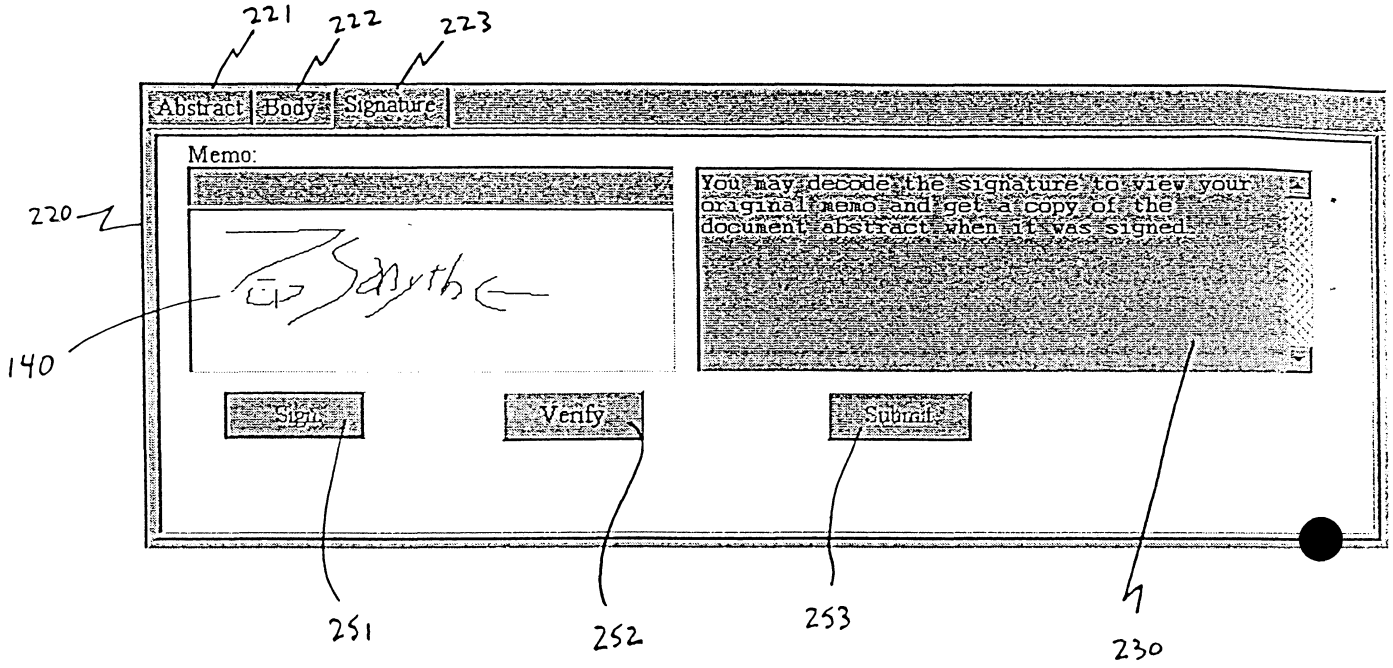
第 6 圖


221
222
223
Abstract
Body
Signature
Memo:
Your private memo and the document abstract have been encoded into your signature for later reference. Press the "Submit" button to submit the signed document to the originator.
220
228
Sign
Verify
Submit
251
252
253
230

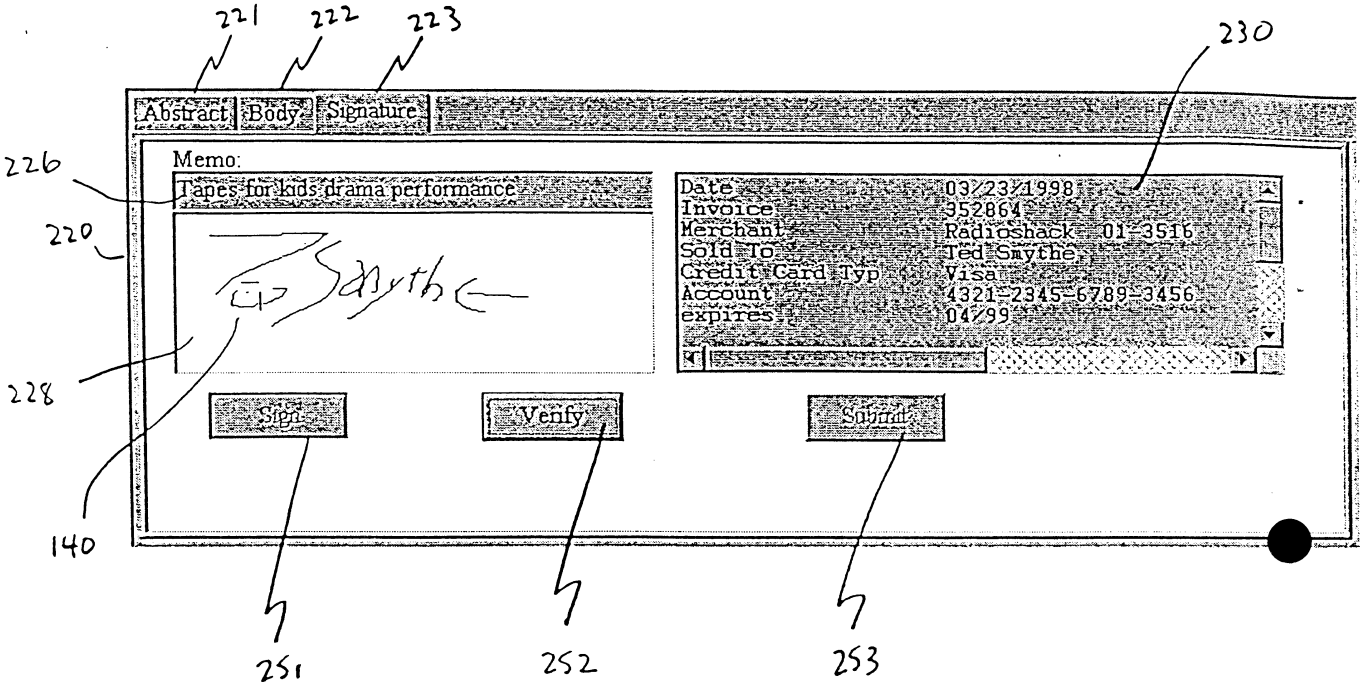
第 7 圖


簽名驗證流程
文件簽名
數位圖形軟體
數位文件
數位圖形簽
發送訊息
公眾鎖鑰 152
秘密鎖鑰 154
150 要求簽名確認及備忘資料解譯
要求文件與簽名連結之確認
153 使用秘密鎖鑰解開備忘資料
155 使用公眾鎖鑰解開摘要
157 將文件摘要與解開後之摘要進行比對
159 顯示備忘文字
161 顯示摘要文字或警告訊息
Secret key
Public key
解開備忘資料、綠色色彩值
Encrypted memo, green color values
Encrypted abstract, blue color values
document abstract
文件摘要
Decrypted memo text
解開後之備忘文字
abstract comparison
摘要比對

第 8 圖

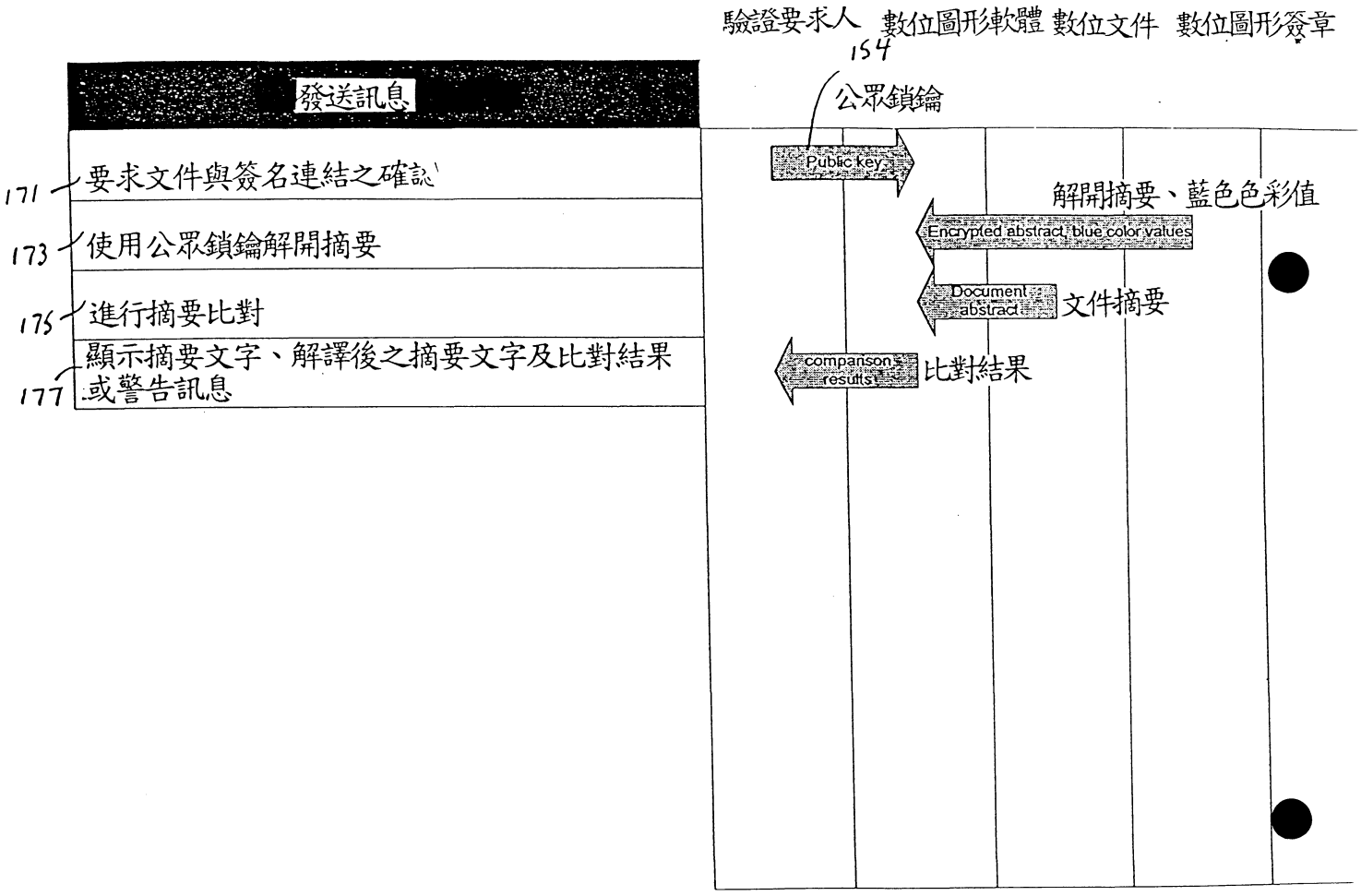

221
222
223
Abstract
Body
Signature
Memo:
You may decode the signature to view your original memo and get a copy of the document abstract when it was signed.
220
140
Sign
Verify
Submit
251
252
253
230

第 9 圖


221
222
223
230
Abstract
Body
Signature
226
Memo:
Tapes for kids drama performance
220
Date 03/23/1998
Invoice 952864
Merchant Radioshack 01-3516
Sold To Ted Smythe
Credit Card Typ Visa
Account 4321-2345-6789-3456
expires 04/99
228
Sign
Verify
Submit
140
251
252
253

第 10 圖

公眾簽名驗證流程



第 11 圖

五、發明說明（24）

印記可以配合傳統之session鎖鑰，以加強安全性。這特別利於在保持內容處於編譯之狀況下，並防止其在接收到時立刻顯現。

舉例來說，銀行客戶可能會希望能夠在網路上更改他們的ATM PIN碼。文件將會包含一摘要，此摘要可能只是說明這是客戶的指示。由於ATM PIN碼之改變是一個短訊息，印記只需要有帳戶號碼、舊PIN碼及新PIN碼被編入紅色色彩值中。在使用了某種編譯技術後，編譯之強度很高，發送至將可以被證實，而且只有設定之接收者可以看見交易之細節。摘要將會提供銀行之處理中心足夠之資訊將此印記送至一安全的環境以解開並處理此交易，不會洩露交易之內容。

本發明雖已以較佳實施例揭露如上，但其並非用以限制本發明。任何熟悉此技藝者，在不脫離本發明之精神和範圍內，當可做些許之更動與潤飾。因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

元件符號說明

2~可見圖像；	4~綠點；
6~紅點；	8~藍點；
102、200~文件摘要；	104~私人鎖鑰；
106~私密備忘資料；	108~私密對稱鎖鑰；
103~非對稱編譯引擎；	107~對稱編譯引擎；
110~圖形簽章墨跡；	111~編譯摘要位元；
112~色點；	113~編譯備忘位元；

五、發明說明（25）

114~單體；　　124~摘要與實體；

126~摘要與實體；　　132~圖形簽名與備忘資料；

134~文件與數位圖形；140~簽名；

202~細節；　　204、214、224~視窗；

210~文件實體；　　220~簽署人界面；

221~摘要；　　222~實體；

223~簽名；　　226~備忘區；

228~圖形簽章區；　　230~備忘資料輸入區；

251~簽下按鈕；　　252~確認按鈕；

253~送出按鈕；　　304~私人通訊；

306~發送者之私人鎖鑰；

308~非對稱編譯引擎；310~接收者之公眾鎖鑰；

312~非對稱編譯引擎。

六、申請專利範圍

1. 一種數位圖形簽章，應用於一個人之交易中，該數位圖形簽章具有一可見圖像，該圖像具有複數圖點，該數位圖形簽章包括：

複數具有至少一第一色彩之合併圖點，代表交易之細節資料，以及複數具有至少一第二色彩之合併圖點，代表該個人之簽章資料，該等合併圖點形成一該個人簽章之可見圖像。

2. 如申請專利範圍第1項所述之數位圖形簽章，其中該交易細節資料包括至少以下之一：

被簽署文件之摘要；

被簽署文件之實體；

被簽署文件之摘錄；

一關於被簽署文件之個人註記。

3. 如申請專利範圍第2項所述之數位圖形簽章，其中該交易細節資料包括該摘要。

4. 如申請專利範圍第3項所述之數位圖形簽章，其中該摘要包括該個人簽署文件後所同意事項之摘錄。

5. 如申請專利範圍第3項所述之數位圖形簽章，其中該摘要包括至少以下參考資訊之一：日期、所牽涉之各方、或交易編號。

6. 如申請專利範圍第3項所述之數位圖形簽章，其中該摘要係以文字呈現。

7. 如申請專利範圍第2項所述之數位圖形簽章，其中該交易細節資料包括被簽署文件之內容摘要。

8. 如申請專利範圍第3項所述之數位圖形簽章，其中

六、申請專利範圍

該交易細節資料包括被簽署文件之內容摘要。

9. 如申請專利範圍第7項所述之數位圖形簽章，其中該摘要係以文字呈現。

10. 如申請專利範圍第2項所述之數位圖形簽章，其中該交易細節資料包括被簽文件之內容。

11. 如申請專利範圍第2項所述之數位圖形簽章，其中該交易細節資料更包括一個人註記。

12. 如申請專利範圍第11項所述之數位圖形簽章，其中該個人註記包括交易之目的、交易之性質或其他對該個人具有重要性之細節。

13. 如申請專利範圍第3項所述之數位圖形簽章，其中該交易細節資料更包括一個人註記。

14. 如申請專利範圍第1項所述之數位圖形簽章，其中該個人簽章資料包括由一個人簽章圖形所產生之圖形資料。

15. 如申請專利範圍第1項所述之數位圖形簽章，其中該交易細節資料及該個人簽章資料是被編碼的。

16. 如申請專利範圍第1項所述之數位圖形簽章，其中該合併之圖點係經色彩編碼。

17. 如申請專利範圍第13項所述之數位圖形簽章，其中該交易細節資料及該個人簽章資料係經色彩編碼，且該摘要包括藍色值，該個人註記包括綠色值而該個人簽章資料包括紅色值。

18. 如申請專利範圍第1項所述之數位圖形簽章，其中該可見圖像能夠被顯示在一視訊顯示終端上。

六、申請專利範圍

19. 如申請專利範圍第1項所述之數位圖形簽章，其中更包括一數位圖形印記，以至少該等色彩之一進行編碼。

20. 一數位圖形簽章系統，包括：

申請專利範圍第1項所述之數位圖形簽章；

一第一輸入裝置，用以輸入該交易細節資料；

一第二輸入裝置，用以輸入該簽章資料；

一視訊顯示終端。

21. 一種產生數位圖形簽章之方法，該數位圖形簽章係相對於一個人所簽署之一文件，該方法包括：

產生一該文件之摘要；

取得一該個人之簽章；

從該摘要產生一文件摘要資料流；

從該簽章產生一簽章資料流；

將該文件摘要及簽章資料流合併為一數位圖形簽章。

22. 如申請專利範圍第21項所述之方法，其中更包括：

取得該個人之備忘資料；

產生一文件備忘資料流；

將該文件摘要、文件備忘及簽章資料流合併為一數位圖形簽章。

23. 一種產生數位圖形簽章之方法，該數位圖形簽章係相對於一個人所簽署之一文件，該方法包括：

選擇與該文件有關之細節；

產生一該文件之摘要；

取得一該個人之簽章；

六、申請專利範圍

從該細節產生一文件細節資料流；

從該摘要產生一文件摘要資料流；

從該簽章產生一簽章資料流；

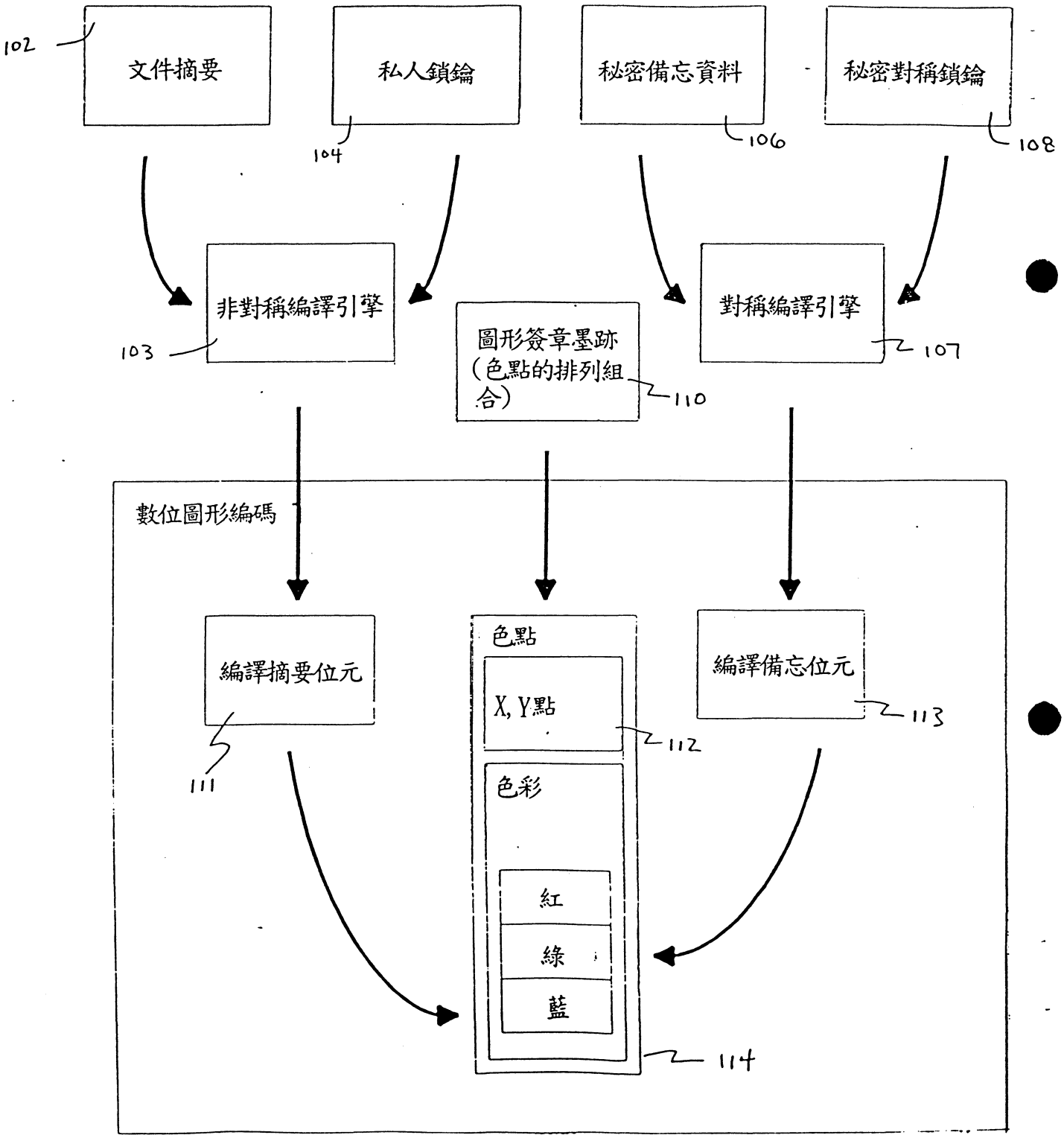
將該文件細節、文件摘要及簽章資料流合併為一數位圖形簽章。

24. 如申請專利範圍第23項所述之方法，其中更包括：

取得該個人之備忘資料；

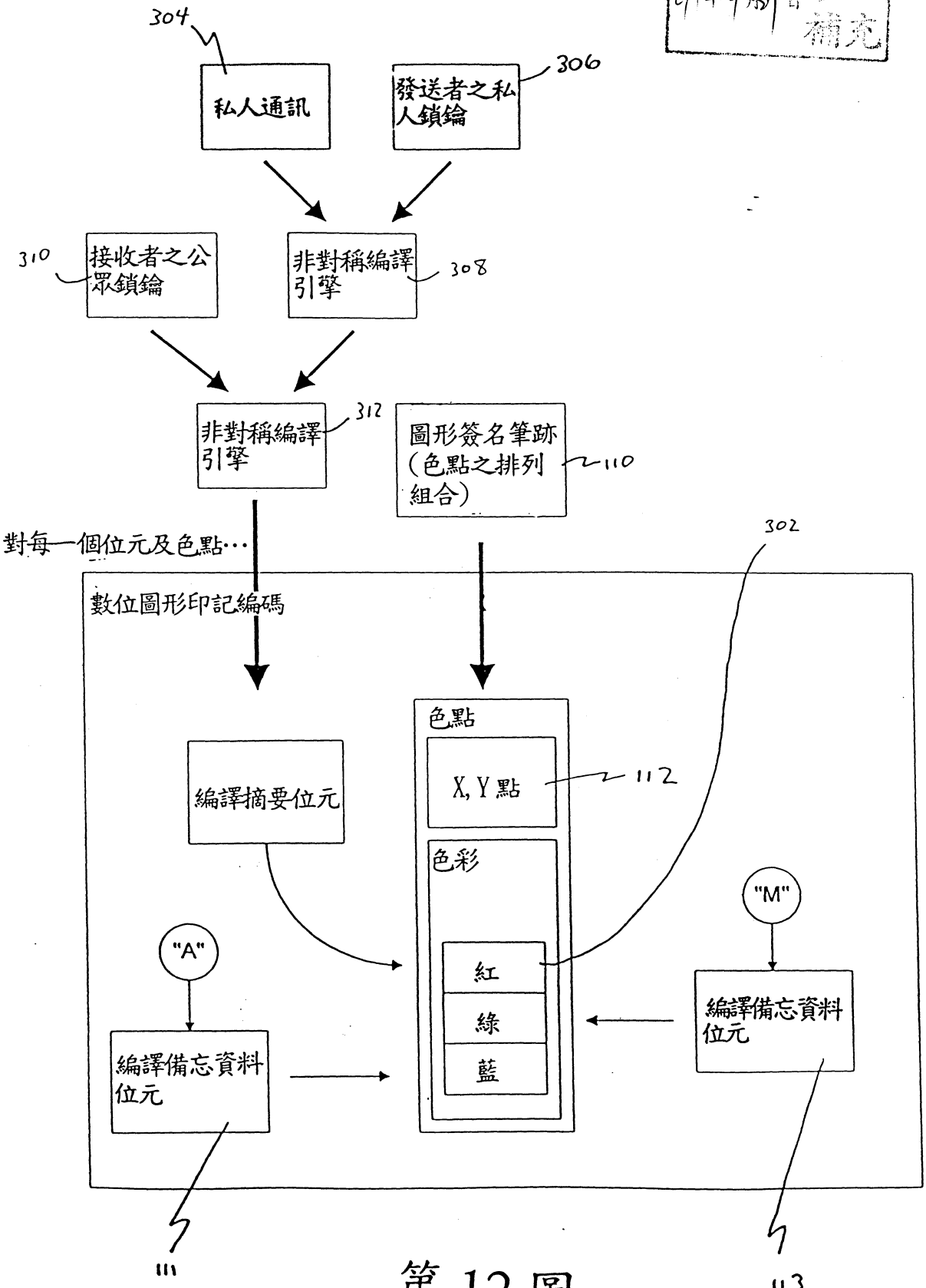
產生一文件備忘資料流；

將該文件細節、文件摘要、文件備忘及簽章資料流合併為一數位圖形簽章。


102
文件摘要
私人鎖鑰
104
秘密備忘資料
106
秘密對稱鎖鑰
108
非對稱編譯引擎
103
對稱編譯引擎
107
圖形簽章墨跡
(色點的排列組合)
110
數位圖形編碼
編譯摘要位元
111
色點
X, Y點
112
色彩
紅
綠
藍
114
編譯備忘位元
113

第 2 圖

91年9月17日 修正補充



第 12 圖