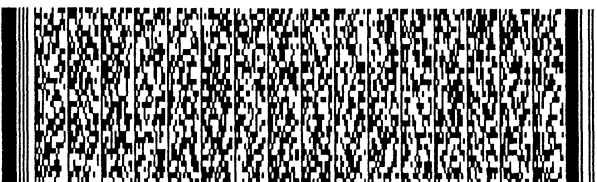


公告本

申請日期：89.4.20	案號：88107470
類別：H04LP/00	

(以上各欄由本局填註)

發明專利說明書		532022
一、 發明名稱	中文	用以插入及驗證數位簽名於數位資料之方法和裝置
	英文	METHOD AND DEVICE FOR INSERTING AND AUTHENTICATING A DIGITAL SIGNATURE IN DIGITAL DATA
二、 發明人	姓名 (中文)	1. 英吉瑪 J. 寇克斯 2. 馬修 L. 米勒 3. 道格拉斯 P. 瑞納
	姓名 (英文)	1. INGEMAR J. COX 2. MATTHEW L. MILLER 3. DOUGLAS P. RAYNER
	國籍	1. 美國 2. 美國 3. 美國
	住、居所	1. 美國新澤西州勞倫斯村市李帕克大道21號 2. 美國新澤西州普林斯敦市奎瑞街12號 3. 美國加州三藩市鑽石街74號
三、 申請人	姓名 (名稱) (中文)	1. 美商NEC公司
	姓名 (名稱) (英文)	1. NEC USA, INC.
	國籍	1. 美國
	住、居所 (事務所)	1. 美國新澤西州普林斯敦市獨立大道4號
	代表人 姓名 (中文)	1. 提摩希 M. 都諾凡
	代表人 姓名 (英文)	1. TIMOTHY M. DONOVAN
		

本案已向

國(地區)申請專利

美國 US

申請日期

1999/04/20 09/294, 956

案號

主張優先權

有

有關微生物已寄存於

寄存日期

寄存號碼

無



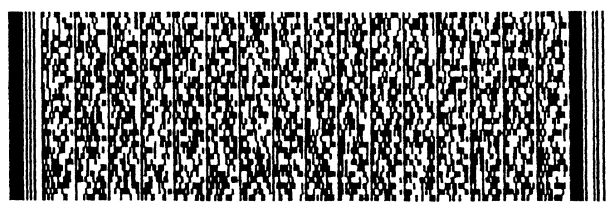
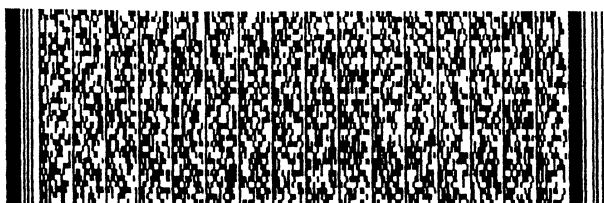
五、發明說明 (1)

本發明有關用以插入及驗證數位簽名於數位資料和，尤其特別的是，用以插入與驗證數位簽名和相關資料於數位影像、連續影像、以及聲音資料中之編碼器與解碼器之方法和裝置。

照片、音樂與連續影像逐漸地以數位化表現，有許多理由包括改良的影像或是聲音品質以及更經濟的分配能力。然而，數位資料內容擁有者(以下簡稱為"內容擁有者")逐漸地了解盜版的相關風險，以及許多的努力朝向降低此風險。數位浮水印為接收注意以降低風險之工具其中一種，早期注目焦點在於不可見的浮水印設計，但仍存在許多例如MPEG-2或JPEG壓縮之常見的信號處理形式。

在技藝中可了解也有一種易消失的浮水印需求，例如浮水印並未存在簡單的影像處理操作。這些易消失浮水印的目的為以一影像是否已經變更之指示提供瀏覽器，數位影像的完整逐漸地受到注目，因為許多低成本軟體系統允許非常複雜的、可無缺點地修改影像之影像編輯能力，目前認為照片是最好的證據以支持此說法。然而這種情形可能改變，假如廣泛的影像"編修"能力導致一般大眾變得對於影像之驗證容易起疑心。

以上這些爭論都在本技藝中獲得解決，解決方案根據驗證可以清楚地了解之傳統密碼法。在密碼法驗證之後的基本想法為透過單方向散列功能傳遞資料以造成N位元散列，使用一公用鑰匙加密編譯演算法之專用鑰匙加密編譯N位元散列以形成數位簽名。為了驗證資料，疑問中之資料



五、發明說明 (2)

再次散列並且此N位元序列與使用相關的公用鑰匙解譯之數位簽名作比較。

此系統之缺點為當其一開始時推薦影像資料作為兩個檔案需求時，一個包含影像而另一個包含簽名。驗證需要兩個檔案的存在，其中可能為一個妨礙，例如因為非常容易地傳送影像但卻忘了傳送相關的簽名。理論上，單一檔案即可滿足，一個明顯的解決方案將連接簽名進入影像檔案格式檔案頭。然而，當影像介於不同檔案格式如tiff、bmp等轉變時，此解決方案是有疑問的。

近來，Wong博士[P.H. Wong "用以影像對比與驗證之公用鑰匙浮水印"，Int. Conf. On影像處理，455-459，1998年10月]提倡一直接的方法以插入簽名功能於影像中，這樣的系統具有不受影像檔案格式改變的優點，以及無須任何meta-資料之格式。在獨立的影像方塊上執行驗證，對每一個方塊而言， X_r ，每個畫素最低有效位元設定為0，此修改過的方塊跟原始影像之寬度與高度資訊一起通過散列功能。此散列功能的輸出以相關的位元集排除的或(XOR'ed)集合， B_r 形成簽名， W_r 為加密編譯的公用鑰匙以形成 $C_r = E_k(W_r)$ ， C_r 插入於方塊之最低有效位元(LSB)以形成浮水印影像方塊 Y_r 。Wong指出 B_r 為二元影像或模型，其尺寸必小於或等於散列之長度。XOR的目的是為了密碼化二元影像， B_r 。隨後在解碼時，每個方塊之LSB平面經由使用相關的公用鑰匙解譯，且在設定方塊之最低有效位元為0之後以方塊的散列予以XOR。假如方塊為真實的，也就

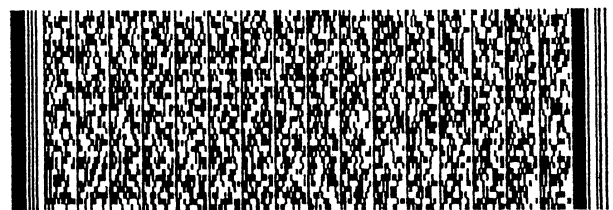
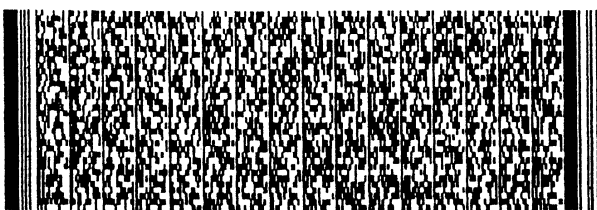


五、發明說明 (3)

是不可改變的，則結果再度為 B_r ，也就是使用相同的散列值XOR第二次之後以反密碼化模型 B_r ，否則模型仍保持密碼形式。影像驗證經由視覺上檢查模型 B'_r ，然而實際上，電腦能執行 B_r 以及 B'_r 位元方式的比較。嚴格而言，這樣的架構只能驗證每個畫素最高有效位元，因為LSB已經改變以便能負載相關的已加密編譯的簽名。

本技藝中其他部分描述了這樣的情形，其中正確的所有權無法經由浮水印的直接應用而再次解決。特別的是，藉由插入偽造浮水印過程，他們確認無人能聲稱浮水印影像所有權之情況，對此問題他們提供一使用稱之為"非反轉"浮水印方法之解決方案，此方法的基本想法為根據原始影像之非反轉功能建構浮水印。一個非反轉功能範例為普遍使用於密碼法之單方向散列功能，這樣的機能花費一連串位元當作輸入，且輸出一有限值，例如1000位元輸出。然而舉例的1000位元輸出，決定相關的輸入是計算上地不可實行的。請注意像這樣的浮水印僅能經由內容擁有者或擁有原始影像者或是其散列鑰匙而讀取。如此一來，一個公用的浮水印，也就是一個可被任何人讀取的浮水印，並不能反轉或是至少損失了非反轉的獲益，因為所有的讀取者必須具有散列值的知識。

進一步而言，使用前述技藝之方法與裝置以驗證隨後將壓縮的以及稍後將解壓縮的影像是麻煩的，從存在JPEG壓縮之驗證架構的透視圖，技藝中的許多地方已經注意照這個問題。也就是說，經由壓縮的減損當數位資料改變時，



五、發明說明 (4)

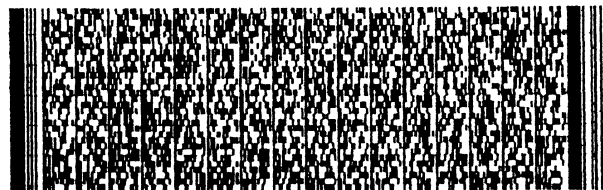
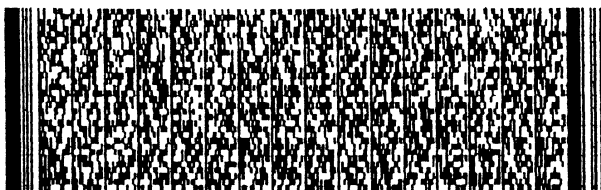
影像本質上還是相同的。

在本發明之方法與裝置中，插入簽名於用以驗證數位資料之數位資料之預定位元中，另一方面，數位資料與部分相關資訊一起驗證。此相關資訊其中可能包括版權注意事項、擁有者辨認。此資訊可能以許多方式嵌入於影像中，如同在浮水印文獻中所討論的情形，嵌入在簽名之前執行（經由散列以及加密編譯創造數位簽名）。

在某一本發明的方法與裝置版本中，我們關心的情形為，對於驗證系統而言壓縮演算法是熟悉的，此方法應用於，例如JPEG壓縮影像或MPEG壓縮連續影像。特別的是，本方法應用於在數位攝影機或其他影像產生裝置內之驗證問題，雖然解決方案並不侷限於這種情形。解析度1Kx1K的數位攝影機產生非常大量必須儲存，以及可能須從攝影機傳送至電腦之資料。為了加速此過程，減少儲存和頻寬的需求，資料將被壓縮是理所當然的。然而當影像最後解壓縮時，瀏覽器必須仍能驗證影像。

在另一本發明的方法與裝置版本中，不僅是數位簽名資料用於驗證目的，而且將時間予以標籤以便為了證明時間的起源。本系統更進一步的精確化為，以影像產生裝置的時間和地點以便時間標籤化影像，後者地點資訊最好透過全球衛星定位(GPS)接收器使用之。

因此，用以插入數位簽名於數位資料中之方法便提供了出來，數位資料包括位元以及包含以下步驟之方法：指定用以接收數位簽名之數位資料預定位元；簽署不包含造成



五、發明說明 (5)

數位簽名之預定位元的數位資料；以及插入數位簽名於數位資料之預定位元，以便驗證隨後的數位資料。

同時提供的是用以在數位資料預定位元中，具有嵌入的數位簽名之驗證數位資料之方法。此方法包含的步驟有：從預定位元選取數位簽名；從造成第一散列之數位資料解譯數位簽名；應用一單方向散列功能施於排除了造成第二散列之預定位元之數位資料上；以及比較第一散列與第二散列，其中假如第一散列與第二散列相符時，則數位資料為已驗證。

在一較佳的本發明之方法與裝置版本中，簽名步驟包括：應用一單方向散列功能施於排除了造成散列之預定位元之數位資料上；以及加密編譯散列。

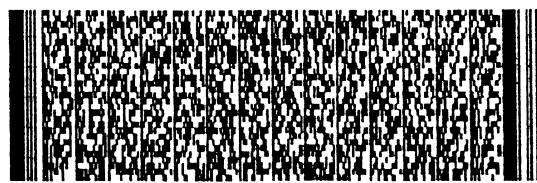
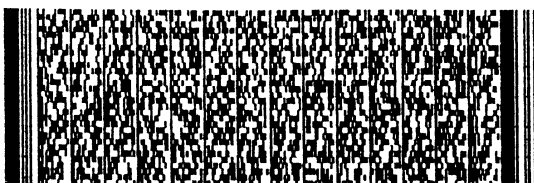
在另一較佳的本發明之方法與裝置版本中，方法進一步包括在簽名步驟之前插入相關資料於數位資料中等步驟，如此一來數位簽名驗證相關資料與數位資料。較佳的是，相關資料插入於排除了預定位元之數位資料位元中。

同時，提供編碼器與解碼器以便執行本發明的方法。

關於下列描述、申請專利範圍、與附圖，本發明中之方法的這些以及其他特徵、方面、與優點將變得更容易了解。其中：

圖1A圖示出數位影像或數位連續影像序列之影像圖框，其中影像或影像圖框包括定義多個畫素之數位資料。

圖1B圖示出表示位元之圖1A之影像或影像圖框，位元包括從最高有效位元到最低有效位元之每個畫素。



五、發明說明 (6)

圖1C圖示出從最高有效位元平面到最低有效位元平面所表示位元平面之圖1A之影像或影像圖框。

圖1D圖示出圖1A之影像或影像圖框，其中數位資料轉變為具有高和低頻率元件之頻率領域。

圖1E圖示出從最高有效位元平面到最低有效位元平面所表示位元平面之聲音數位資料。

圖2A為圖示出一插入數位簽名於本發明之數位資料中之較佳方法流程圖。

圖2B為圖示出驗證具有嵌入數位簽名於數位資料預定位元中之數位資料之較佳方法流程圖。

圖3為一用以簽名以及/或是標籤化數位資料，以便驗證隨後的數位資料和時間標籤之裝置架構圖。

圖4為一用以插入資料於數位資料之裝置概要圖，該數位資料具有用以接收來自外部資源之裝置。

圖5為一用以插入資料於數位資料之裝置概要圖，該數位資料具有辨識的裝置，以辨識裝置的使用者，並且插入的資料為一辨認裝置使用者之辨認器。

雖然本發明應用於各種類型數位資料，曾經發現於使用數位攝影機所產生的數位影像資料環境中特別有效。因此，不限本發明應用於影像資料或數位攝影機，本發明將於上述的環境中描述出來。然而，技藝中這些平常的技術將認識到本發明之方法與裝置相同地應用於數位連續影像和數位聲音資料，以及任何形式之資料產生裝置。

在討論本發明之前，參考圖1A至1D以討論簡要的概觀數

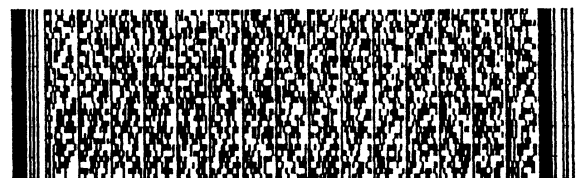
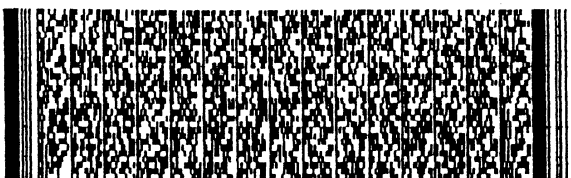


五、發明說明 (7)

位影像。圖1A圖示出數位影像100，數位影像100可能是來自數位影像中之影像圖框序列之影像圖框，數位影像經由多個影像畫素102表示出來，其中畫素以影像100右下角圖示出來。現在請參考圖1B，每個畫素經由多個位元104定義，從人類視力最容易可見之最高有效位元(MSB) 106，到人類視力最難看見之最低有效位元(LSB) 108。如圖1C中所見，構成影像100之畫素其相關的位元形成一個位元平面，影像畫素102之所有最高有效位元106構成最高有效位元平面110。同樣地，影像畫素102之所有最低有效位元108構成最低有效位元平面112。圖1E圖示在一段時間系列中相關的數位資料，例如聲音資料。聲音數位資料以樣本(行)124表示，其中每個樣本是由最高有效位元106到最低有效位元108表示，在此相關位元的列以平面視之，從最高有效位元平面110到最低有效位元平面112，即使它們是單獨的列。

以定義畫素之位元的意義狀態表示之影像100，表現方式為單方向地表示數位資料如影像般。通常數位資料包括多個樣本、每個樣本經由多個位元所定義，其中樣本為影像資料之畫素、聲音資料之時間標籤、以及連續影像資料之空間性暫時樣本。此方法則將位元轉變為至少具有第一和第二特徵元件之另一種表現方式。預定位元包括第一和第二特徵元件之一種，假如也插入相關資料，則相關資料會至少插入第二特徵元件之一部分。

一種定義影像的方法為，將數位資料轉變為頻率領域



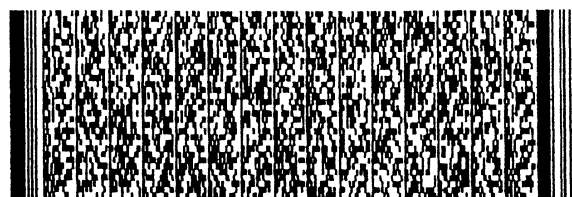
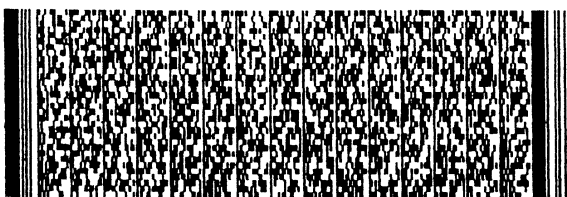
五、發明說明 (8)

114，如圖1D所示。在頻率領域中，影像100分別轉變為高頻率元件116和低頻率元件118，高頻率元件116比低頻率元件118在人類視力上較為不可見。較佳地，預定位元包括一部分高頻率元件，且假如有的話，任何相關資料插入於剩餘高頻率元件以及/或是低頻率元件。

需要簽署(插入一數位簽名)或驗證影像100之位元數是非常小的，最好介於128與256之間，當與512x512x24傳統影像比較時上述情況特別是真實的，傳統上數位簽名插入於LSB平面中，因為對於人類視力而言是最難看見的平面。然而，完全不需要改變所有影像100之最低有效位元，只有一部分LSB平面120需要經由插入數位簽名而改變。如此一來，插入LSB平面之120部分之簡單簽名程序，以最少改變原始影像方式提供一基本驗證程序。

本發明之基本插入方法以圖2A中之部分步驟圖示出來。在步驟200中，提供定義數位影像(或其他選擇，數位連續影像或聲音)之數位資料。在步驟202中，數位資料之預定位元指定給隨後插入之數位簽名。較佳地，預定位元包括至少一部分LSB平面120，然而數位資料的任何部分都能指定為預定位元，預定位元數最好與數位簽名中之位元數是相同的。不過，預定位元數能選擇性地比數位簽名大小來得大，以允許插入更多的數位簽名或其他資料。

接下來，簽署排除了造成數位簽名之預定位元之數位資料，技藝中任何已知的簽名方法能在不脫離本發明之範圍與精神下使用。較佳地，經由首先應用一單方向散列功能

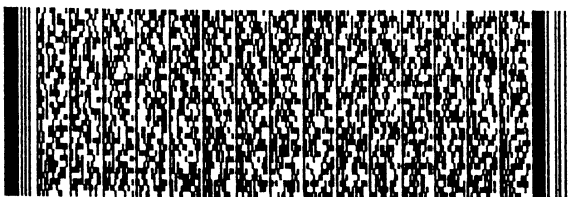


五、發明說明 (9)

於排除了造成散列(或散列值)之預定位元之數位資料上以完成簽名，步驟210展示了上述情形。在步驟220加密編譯散列造成數位簽名，數位簽名在步驟226插入數位資料之預定位元，圖2A流程圖所圖示出之剩餘步驟對於前述討論的方法而言是較好的或是另一種選擇。

一旦數位簽名已經插入於預定位元時，用以驗證數位資料之本發明基本方法，將參考圖2B討論之。在步驟228數位簽名從已知的預定位元120位置選擇出來。在步驟230，從造成第一散列之數位簽名解譯出數位簽名。在步驟232，用以編碼數位資料之已知單方向散列功能應用於排除了造成第二散列之預定位元之數位資料。在步驟234，比較第一散列和第二散列，且有一判斷二者是否相符之決定。假如第一散列和第二散列相同時(步驟238)，則驗證數位資料；假如第一散列和第二散列不相同時(步驟240)，則不驗證數位資料。圖2B流程圖所圖示之剩餘步驟為相似於將在後面討論之圖2A部分較佳步驟之較佳步驟。

本方法之限制為其並未配置已經改變之影像區域，確切地說，演算法簡單地宣稱影像已經驗證或尚未驗證，有許多情況其中這是適當的。然而，沿用此方法於方塊基礎方法是簡單的，其中每個方塊是獨立地簽署。進一步而言，簽名不需要放置於影像之LSB之中，主要的特色為影像分割成兩個分離的空間，第一空間須捕捉到需要驗證的主要特色，第二空間為一個更為剩餘的、可能在認知上沒有意義的影像區域。例如，頻率基礎的系統也是可能的，其中

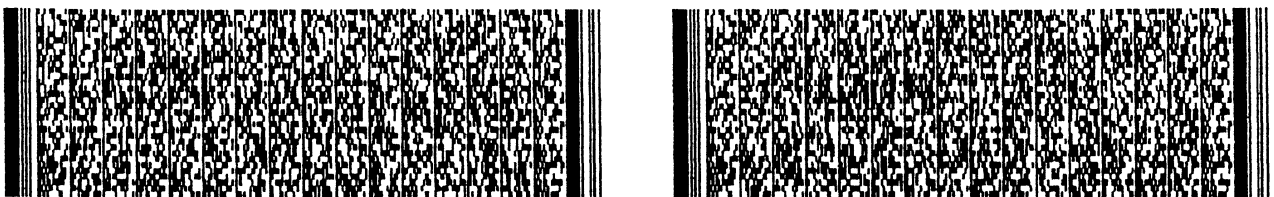


五、發明說明 (10)

影像(或子影像)首先轉變為頻率領域114。接下來,當高頻率(認知上地無意義)係數116用於保留數位簽名時,影像100之低頻率認知上地有意義元件118已經驗證。其他的改變是可能的,包括插入轉變的領域最低有效位元。

當然一般了解的是,對幾乎所有影像LSB之改變並不能辨識。如此一來,其他最低有效位元,例如(512x512x1 - 用於數位簽名之數目)提供一個嵌入或插入更多資訊於影像中(步驟208)之機會,參考相關資料。前述技藝的方法並不能有效地利用這些位元,因為前述技藝方法需要修改一個方塊之所有最低有效位元。本發明之一選擇版本為,簡單地使用大量剩餘位元集以便對影像有關之額外資訊編碼。這樣的資訊可能包括,但卻不僅於此,照相者姓名、版權允許等,公用鑰匙需要去解譯數位簽名、來源或數位資料擁有者,例如錄製數位影像之照相者以及網際網路位址。另一方面,相關資料122可能包括至少兩個部分122a、122b,各具有可能相互獨立或相關而分開的資料。例如,區域122a可能包括辨識用來解譯數位簽名之公用鑰匙,另一區域122b可能包括辨識包含於第一區域122a中之公用鑰匙擁有者。當其他區域正在編碼時,內容擁有者可能選擇以乾淨的,也就是非加密編譯的方式將部分資訊編碼。

較佳地,相關的資料以部分影像對待和簽署。如此一來,不僅驗證了影像內容,並且也驗證相關資訊。相關資訊如圖1C參考數122所示,並最好插入排除了預定位元部分之LSB平面,其中預定位元包含數位簽名。對於技藝中之



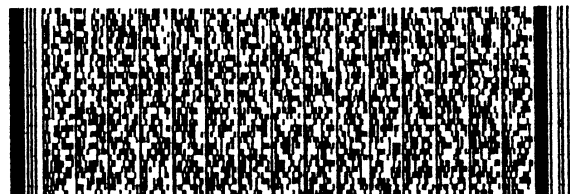
五、發明說明 (11)

技術而言下述情形是明顯的，嵌入相關資料122於LSB平面108之剩餘部分是本發明中之方法最佳實現，並僅能以範例的方式行之。相關資料可能以各種不同方式嵌入，其中許多已經在前述浮水印技藝之中描述過了。

對於技藝中之技術而言下述情形是明顯的，LSB平面類似地存在於其他數位內容形式中。通常數位資料包括多個樣本，其中每個樣本由數位資料中之眾多位元從最高有效位元到最低有效位元定義。在數位影像資料例子中，每個樣本為影像畫素；在數位連續影像中，每個樣本為空間性暫時樣本；而當在數位聲音中時，每個樣本為時間樣本。

在本發明插入方法之另一選擇版本中，數位資料包括多個樣本、聲音、連續影像或影像，在此選擇方案中忽略數位資料中之最低有效位元平面，相關資料連接成具有忽略的最低有效位元平面之數位資料，具有連接的相關資料之數位資料則簽署以造成插入於預定位元之數位簽名。忽略不僅代表最低有效位元平面未通過散列，也代表所有LSB平面之位元設定為0或1，或是任意的模型等等。

本發明的方法並不侷限於簽署完整的數位資料，部分區域也可以簽署。然而，對於部分技藝而言下述情形是明顯的，假如簽名在長度上維持128位元，則當影像分割成N個方塊時有128N位元用來簽名。如此一來，可能在偽造位置處以及可嵌入於影像之大量額外資訊之間有一個交換，特別是假如LSB用來儲存相關資料與簽名。在此限制下，假如每個子方塊僅包括128畫素，就沒有額外容量可用於LSB



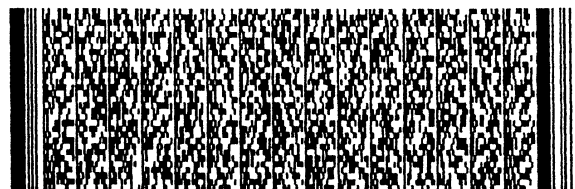
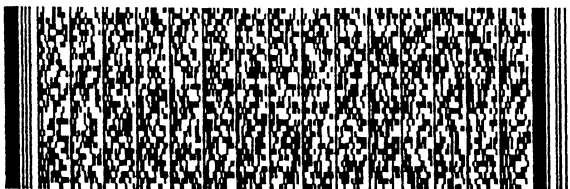
五、發明說明 (12)

平面中。請注意不論如何，當本發明之方法較佳地需要每個子方塊大於或等於散列長度時，Wong需要每個子方塊小於或等於散列長度。

無論資料儲存與傳輸速率非常快速的演變，影像仍需要非常大的頻寬與儲存量。因此，在許多例子中，由於經濟上的原因，內容需要者將需要壓縮數位資料，例如影像用之JPEG，或連續影像用之MPEG。在這種情形下，簽署壓縮影像以及在解壓縮之後具有一簽名影像是令人合意的。

回頭參考圖2A，首先決定的是數位資料是否在步驟204壓縮。假如資料並未壓縮，如前所述本方法接著簽署數位資料。假如數位資料已經壓縮，數位資料在步驟206解壓縮以使得在步驟210和220計算簽名，在步驟222和224數位簽名插入於壓縮檔之檔案頭。較佳地，修改所使用的解壓縮演算法，以使得在影像解壓縮之後目前在檔案頭中之簽名複製到相當的解壓縮影像之預定位元。

現在請參考圖2B，當檔案頭中之數位簽名壓縮檔驗證後，壓縮檔案在步驟242解壓縮，且檔案頭中之數位簽名在步驟244插入於數位資料之預定位元中。假如數位資料也包括相關資料(步驟246，決定方塊之"是")，相關資料可能在步驟224插入於檔案頭，並在步驟242解壓縮之後於步驟248上插入數位資料。另一方面，可在壓縮之前插入相關資料於影像中，並在此方式下相關資料保留壓縮步驟。用以驗證數位簽名(以及假如目前為相關資料)之方法如前所述則為步驟228到240。



五、發明說明 (13)

另一方面，本發明方法之驗證能力延伸到包括時間標籤，其中包括插入時間資料於數位資料以判斷時間數位資料已經創造。回頭參考圖2A，用以時間標籤化數位資料之基本程序如前所述包括首先透過單方向散列功能傳送數位資料，假如數位資料已經時間標籤化(步驟212，決定方塊之"是")，單方向散列功能與簽名傳送至在步驟214連接散列、簽名和時間資料，並在步驟216透過另一個單方向散列傳送散列、簽名和目前時間/日期(時間資料)之可信賴的第三者(third party)。此散列在步驟218使用公用鑰匙加密編譯方法密碼與加密編譯簽名編譯之，並且時間資料回到內容擁有者，如前所述在步驟226簽名和時間資料可再次編碼成為部分數位資料預定位元。在此方式下，證明影像並非偽造的以及決定原始內容必已經存在之日期是可能的。對於技藝中之技術而言下述情形是明顯的，任何技藝中已知之時間標籤程序能在不脫離本發明之範圍與精神下使用。

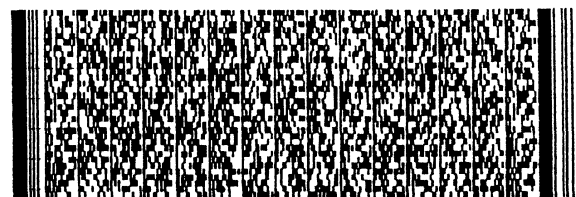
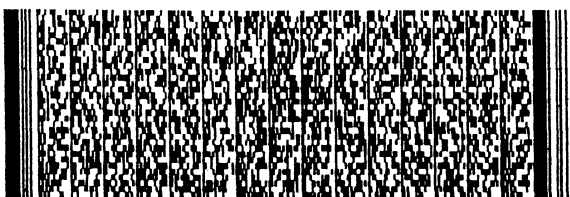
此種安排需要可信賴的第三者標籤組織，傳統上像這樣的組織可在網路上接觸到，例如網際網路。然而，這樣的架構對於經由影像產生裝置產生之即時時間標籤影像並不是實際的，例如由數位攝影機所擷取之影像，因為數位攝影機可能並未接觸到可信賴的第三者。請參考圖3，一個選擇性的安排以便提供每個數位攝影機或是具有數位資料產生裝置301之影像產生裝置300，例如數位掃描器或是數位連續影像攝影機，使用具有防搗毀時鐘304之半導體晶



五、發明說明 (14)

片302與例如能夠執行相同滾動一如可信賴的第三者之公用鑰匙加密編譯系統之防搗毀時間標籤電路306。例如裝置300較佳地具有嵌入於記憶體308中之私密鑰匙，使得它是不可存取的。防搗毀時鐘將在工廠設定並且不能為使用者改變。較佳地，相關的公用鑰匙放置在乾淨的(非加密編譯)影像的LSB範圍之內。使用來自記憶體308之私密鑰匙，經由簽署於裝置303數位資料簽署下來。假如相關資料將插入時，在經由簽署裝置303簽署之前，相關資料插入裝置305插入相關資料於數位資料。相關資料(假如有的話)，簽名以及時間標籤(假如有的話)提供給插入裝置307，以便簽名以及/或是造成簽名之時間標籤以及/或是時間標籤數位資料。

防搗毀硬體也能提供時間以外的資訊，例如參考圖4，影像產生裝置300能夠提供來接收例如來自外部資源402之相關資料，例如GPS(全球衛星定位)接收裝置404如天線之傳送。在這樣的環境中，確認不僅創造時間數位資料(例如取相的時間)，甚至位置是可能的。在這樣的方法下，影像產生裝置300接收將插入之資料，較佳地為RF(射頻)傳送例如從GPS傳送，插入資料於數位資料中，並驗證數位資料以及前述任何插入的相關資料。外部資源也可以為網際網路連接406，其中影像產生裝置400連接具有存取網際網路408，以及能夠接收從網際網路網站傳送資料之個人電腦408。經由記憶卡插槽或連接至個人電腦408之有線裝置412，可從數位攝影機或其他影像產生裝置300下載資



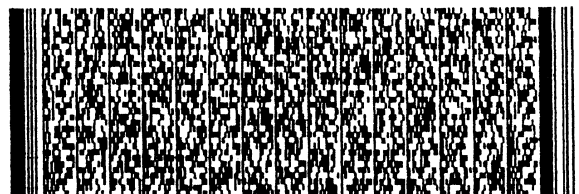
五、發明說明 (15)

料。

在數位攝影機或其他數位內容創造裝置案例中，驗證與時間標籤需要使用公用鑰匙加密編譯系統。裝置使用攝影機私密鑰匙加密編譯簽名以及/或是時間標籤，讀取頭必須具有相關公用鑰匙之知識以便於，就說是，驗證影像吧。然而，有可能上百萬個這樣的裝置存在。一個重要影像LSB的使用為，控制裝置的相關公用鑰匙，例如攝影機，以便於啟動驗證。然而在此時可確定的是，一個特定的攝影機捕捉影像，瀏覽器並不知道是誰擷取了影像。

在前述技藝方法的另一選擇版本中，此知識也能經由允許拍照者(使用者)使用他的/她的名字，以及公用與私密鑰匙程式化他的/她的攝影機(影像產生裝置)而提供。拍照者的名字，就說是亞當吧，與公用鑰匙可能完全地放置於驗證過的影像(數位資料)LSB範圍內。影像，是跟所有的LSB一起的，除了用來儲存簽名的之外，使用私密鑰匙經由攝影機首先簽署。接下來，使用拍照者私密鑰匙加密編譯這個簽名。

可能還有幾種簽名水準，允許經由攝影機(代表在來自CCD陣列記錄之後，資料還沒有處理)、拍照者(辨識負責影像的人)、分配者等，簽署了影像。然而早期簽名水準必須留下可用以提供下一代簽名水準，以及可能相關資料的位元。例如，數位攝影機可能簽署除了LSB平面之所有影像位元，並插入簽名於LSB平面之預測範圍中。接下來，拍照者(在攝影機中或在個人電腦上)可能插入相關資料



五、發明說明 (16)

於LSB平面之其他範圍中，並與來自攝影機之簽名一起簽署這些範圍。第二簽名將放置在另一個LSB平面之預測範圍，可能還有其他運用，提供保留在預定位元中之空間以便儲存簽名。請注意，照相者簽署相關資料以及攝影機計算的簽名。這足以了解照相者擷取影像，即使第二水準簽名並未明確地簽署影像。然而，這是選擇性的方法但並非較佳的具體實施例，因為影像資料第二次散列並非必要地給予來自攝影機之簽名。

請參考圖5，以照相者的公用與私密鑰匙程式化攝影機之更進一步精確化牽涉到提供數位資料產生裝置300，也就是攝影機，提供以例如像是低成本指紋辨識系統之生物辨識系統辨識裝置502。攝影機能以數個照相者之資訊予以程式化，並根據攝影機300所保持的人類指紋選擇正確的一個。

換句話說，如圖3所示具有數位資料產生裝置301或其他編碼裝置之影像產生裝置300，額外地具有辨識裝置502，記憶體308將進一步儲存符合至少一個記憶體308之範圍308a中之裝置使用者之識別號。識別號最好為照相者的名字或是其他像是社會安全碼的識別號。較佳地，相關每個使用者的私密鑰匙儲存於記憶體308之第二範圍308b中。辨識裝置502辨識使用者，其識別號儲存於記憶體308之第一範圍308a中，符合認識的使用者之識別號輸出至相關資料插入裝置305作為相關的資料。較佳地，已辨識的使用者私密鑰匙經由簽名裝置303為了使用而從記憶體308之第



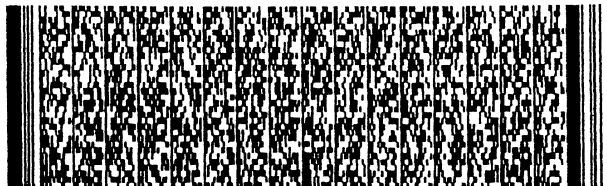
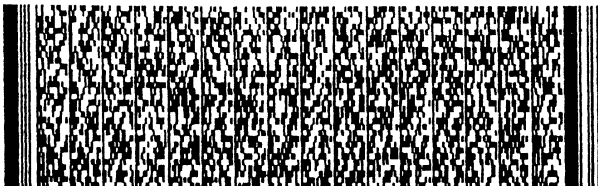
五、發明說明 (17)

二範圍308^b輸出以便簽署數位資料，如此一來可確保資料(影像)絕不再經由第二處理修改或調整。如圖3中之具體實施例所示，相關資料(假如有的話)、時間標籤(假如有的話)、以及簽名提供給插入裝置307，簽名以及/或是造成簽名之時間標籤以及/或是時間標籤數位資料。然而，在隨後的處理之後也簽署數位資料，例如在個人電腦之中。在經由數位攝影機取相數位影像案例中，數位影像首先載入個人電腦中，並以技藝中已知之標準軟體處理，接著簽署，其中處理的影像隨後驗證之。

請注意當較佳具體實施例產生了發生於攝影機內之第二回合加密編譯時，這並非是基本的。例如，經由攝影機簽署之影像可經由照相者^煮下載至個人電腦，其中應用程式將執行第二回合加密編譯。事實上，對於不支援驗證之數位攝影機而言，所有以上程序都能在個人電腦離線時執行。攝影機基礎系統之優點為，在每個照相取得之後自動執行驗證。然而很明顯地，照相者使用個人電腦與相關軟體便能負責地簽署在其工作上。

瀏覽器首先使用照相者之私密鑰匙解譯簽名，此鑰匙是在可用的影像LSB範圍內。使用攝影機公用鑰匙此結果隨即解譯，也同樣是在可用的攝影機LSB範圍內。在此點上，解譯的簽名可與影像與資料之散列比較，以判斷全部的真實性。

假定驗證為負，此點上之瀏覽器僅知道某人宣告亞當為影像來源。然而，並沒有什麼可以阻止某人成為亞當。最



五、發明說明 (18)

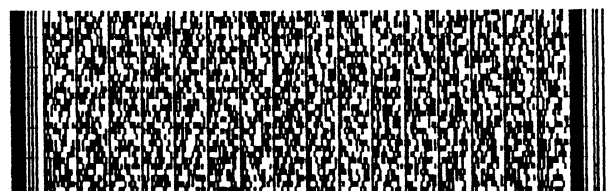
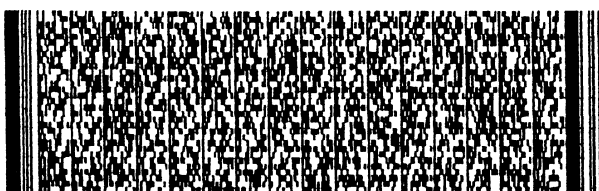
後一步驟因此終歸絕對地確定照相者的確是亞當，瀏覽器必須證實亞當之公用鑰匙的確是亞當的，有許多方式可以完成它，例如可信賴的第三者可能提供列出照相者與其相關公用鑰匙之資料庫，這樣的資料庫可能由一非營利職業照相者或是商業行家提供，這樣的資料庫可能是連線以及/或是定期地像電話目錄般列印。一較不集中解決方式為

可能牽涉在網際網路上存取亞當之網頁。當然，因為他並不知道亞當的私密鑰匙，對他而言便不可能正確地加密編譯簽名，這是公用鑰匙加密編譯系統之一偉大力量。

當了解到照相者擁有許多攝影機時，可發展更進一步的系統精確化。在這樣情況下，照相者希望所有由他所擁有之攝影機使用一與照相者相關之私密鑰匙，這將與每個攝影機所用之個別鑰匙形成一對比。儘管如此，防搗毀晶片也能包括攝影機之序號，藉以確認是哪一個照相者的攝影機實際地照相。

也是而很明顯地，當解譯集中在靜態單張影像時，本方法也能應用於內容之連續影像、聲音資料、與多媒體形式。

雖然已經圖示出以及描述出，何者為本發明之較佳具體實施例所應考慮的，當然能夠了解在不違反本發明之精神下可以做些許形式上或細節處之變動與修改。因此傾向於本發明並未侷限於所描述出來的以及圖示出來的精確的形式，反而應建構成為以涵蓋所有落於申請範圍內之修改。

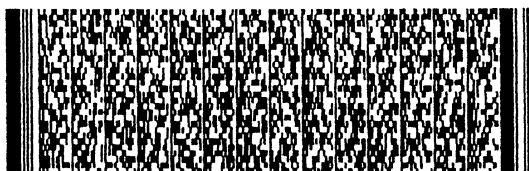
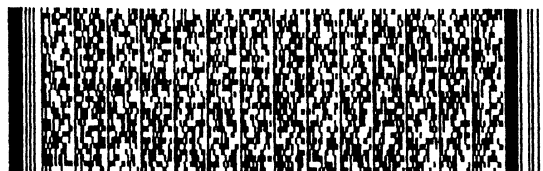


四、中文發明摘要 (發明之名稱：用以插入及驗證數位簽名於數位資料之方法和裝置)

一種用以插入數位簽名於數位資料之方法，該數位資料具有位元且該方法包括指定數位資料之預定位元以接收數位簽名；簽署除造成數位簽名之預定位元以外之數位資料；以及插入數位簽名於數位資料之預定位元，以驗證隨後的數位資料等步驟。同時提供用以驗證於數位資料預定位元中具有嵌入式數位簽名之數位資料等步驟之方法，該方法包括：從預定位元選取數位簽名；從造成第一散列之數位資料解譯數位簽名；經由使用數位資料編碼器應用一已知單方向散列功能施於除造成第二散列之預定位元以外之數位資料上；以及比較第一散列與第二散列，其中假如第一散列與第二散列相符時，則數位資料為已驗證。在本發明之較佳版本方法中，進一步包括早於簽名步驟之前插入

英文發明摘要 (發明之名稱：METHOD AND DEVICE FOR INSERTING AND AUTHENTICATING A DIGITAL SIGNATURE IN DIGITAL DATA)

A method for inserting a digital signature into digital data is provided. The digital data has bits and the method includes the steps of: assigning predetermined bits of the digital data for receiving the digital signature; signing the digital data excluding the predetermined bits resulting in the digital signature; and inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data. Also provided is a method



四、中文發明摘要 (發明之名稱：用以插入及驗證數位簽名於數位資料之方法和裝置)

相關的資料於數位資料中，如此一來數位簽名驗證相關的資料與數位資料。較佳地，相關的資料插入於除預定位元以外之數位資料位元中。

英文發明摘要 (發明之名稱：METHOD AND DEVICE FOR INSERTING AND AUTHENTICATING A DIGITAL SIGNATURE IN DIGITAL DATA)

for authenticating digital data having the embedded digital signature in the predetermined bits of the digital data including the steps of: extracting the digital signature from the predetermined bits; decrypting the digital signature from the digital data resulting in a first hash; applying a known one-way hashing function used by an encoder of the digital data to the digital data excluding the predetermined bits resulting in a second hash; and comparing the



四、中文發明摘要 (發明之名稱：用以插入及驗證數位簽名於數位資料之方法和裝置)

英文發明摘要 (發明之名稱：METHOD AND DEVICE FOR INSERTING AND AUTHENTICATING A DIGITAL SIGNATURE IN DIGITAL DATA)

first hash to the second hash wherein if the first hash matches the second hash the digital data is authentic. In a preferred version of the methods of the present invention, the method further includes the step of inserting associated data into the digital data prior to the signing step such that the digital signature authenticates both the associated data as well as the digital data. Preferably, the associated data is inserted into the bits of the digital data excluding the



四、中文發明摘要 (發明之名稱：用以插入及驗證數位簽名於數位資料之方法和裝置)

英文發明摘要 (發明之名稱：METHOD AND DEVICE FOR INSERTING AND AUTHENTICATING A DIGITAL SIGNATURE IN DIGITAL DATA)

predetermined bits.



圖式

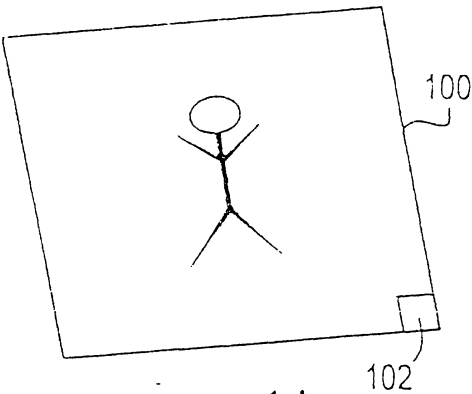


圖 1A

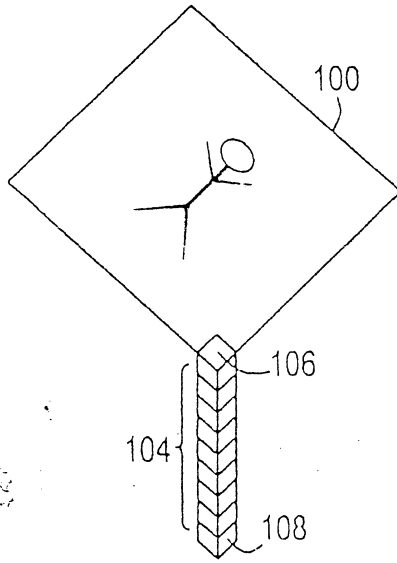


圖 1B

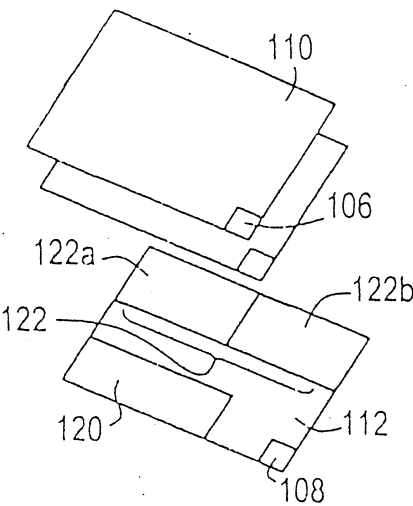


圖 1C

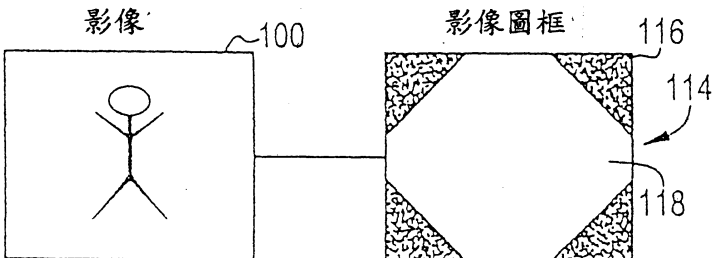


圖 1D

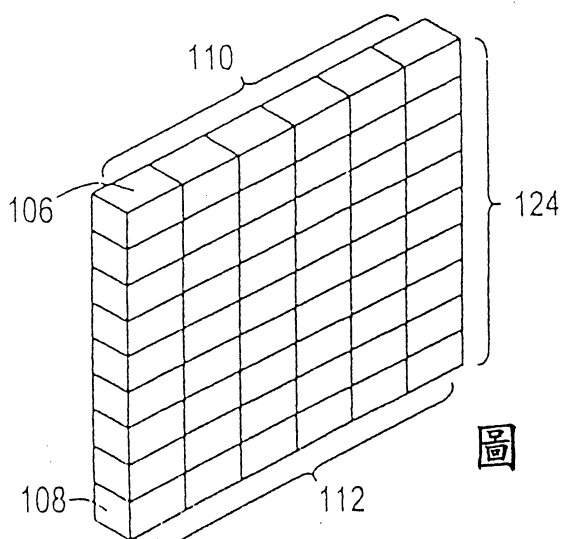


圖 1E

圖式

編碼器

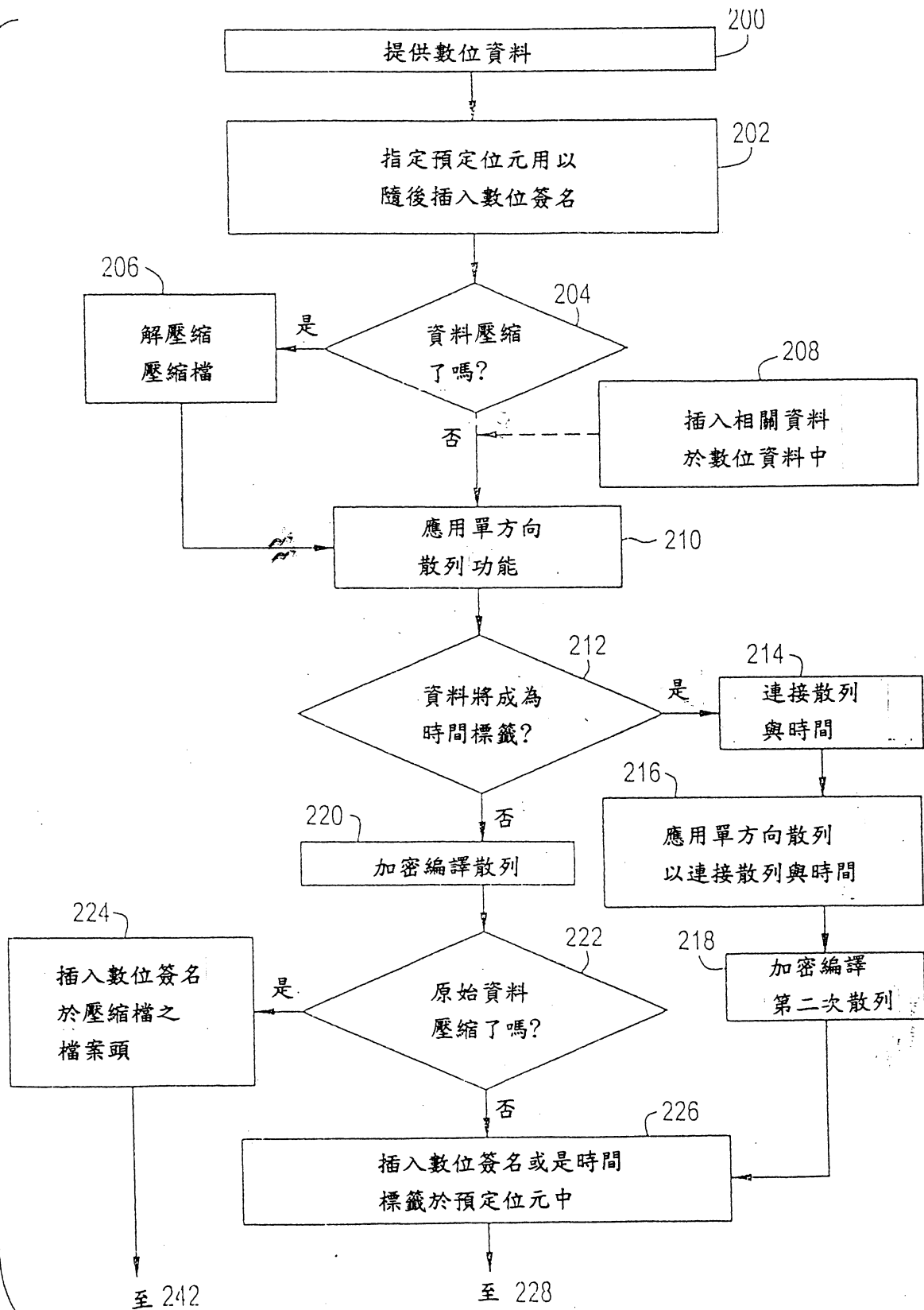


圖 2A

圖式

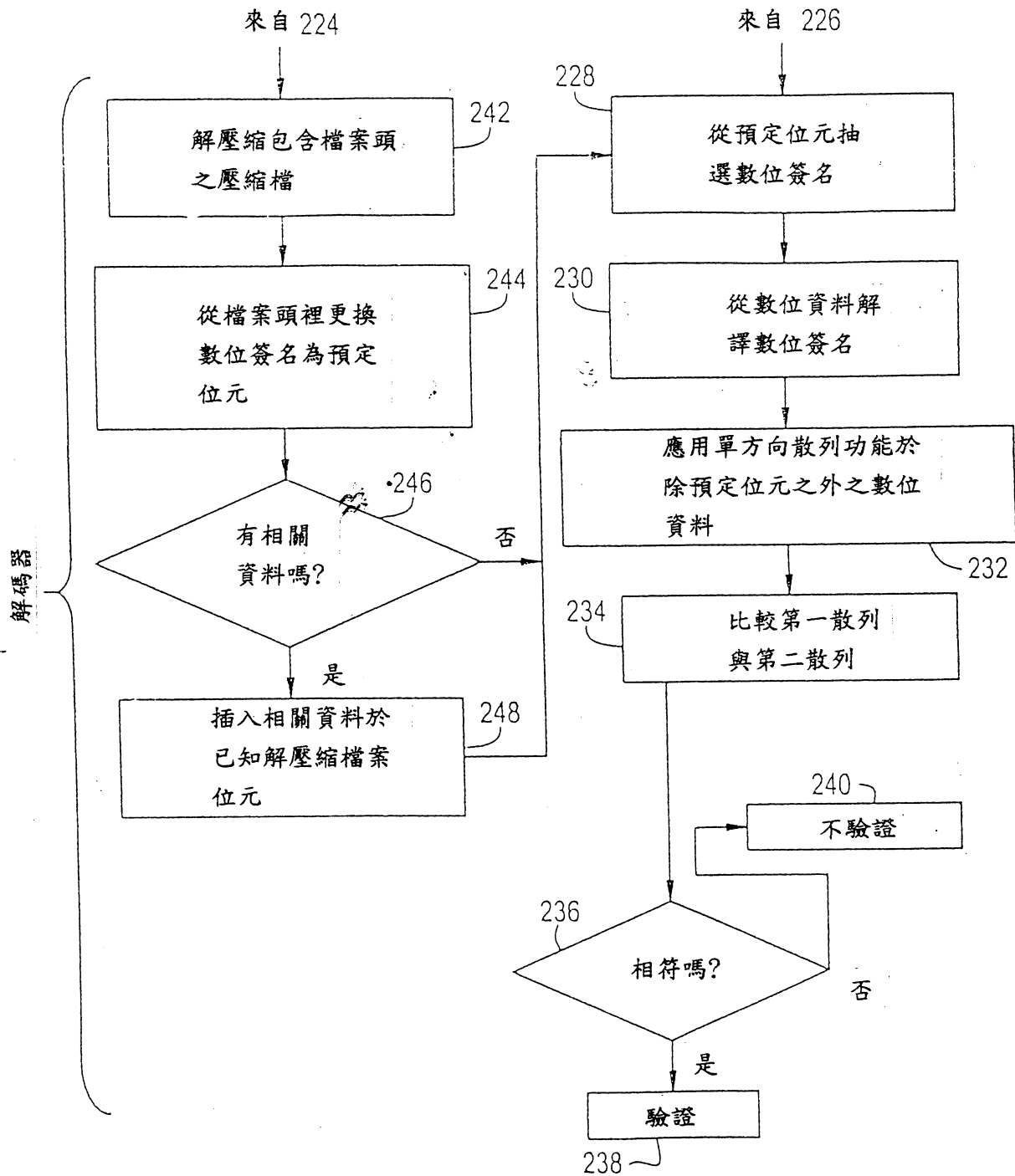


圖 2B

圖式

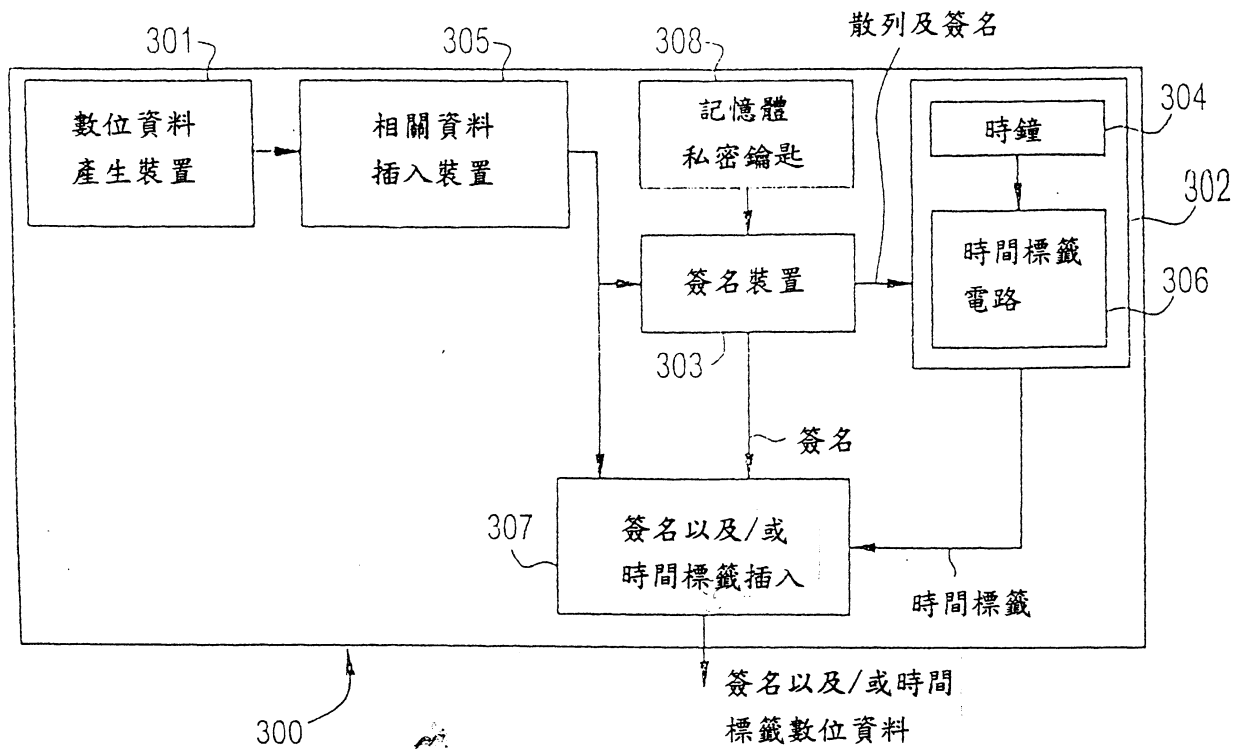


圖 3

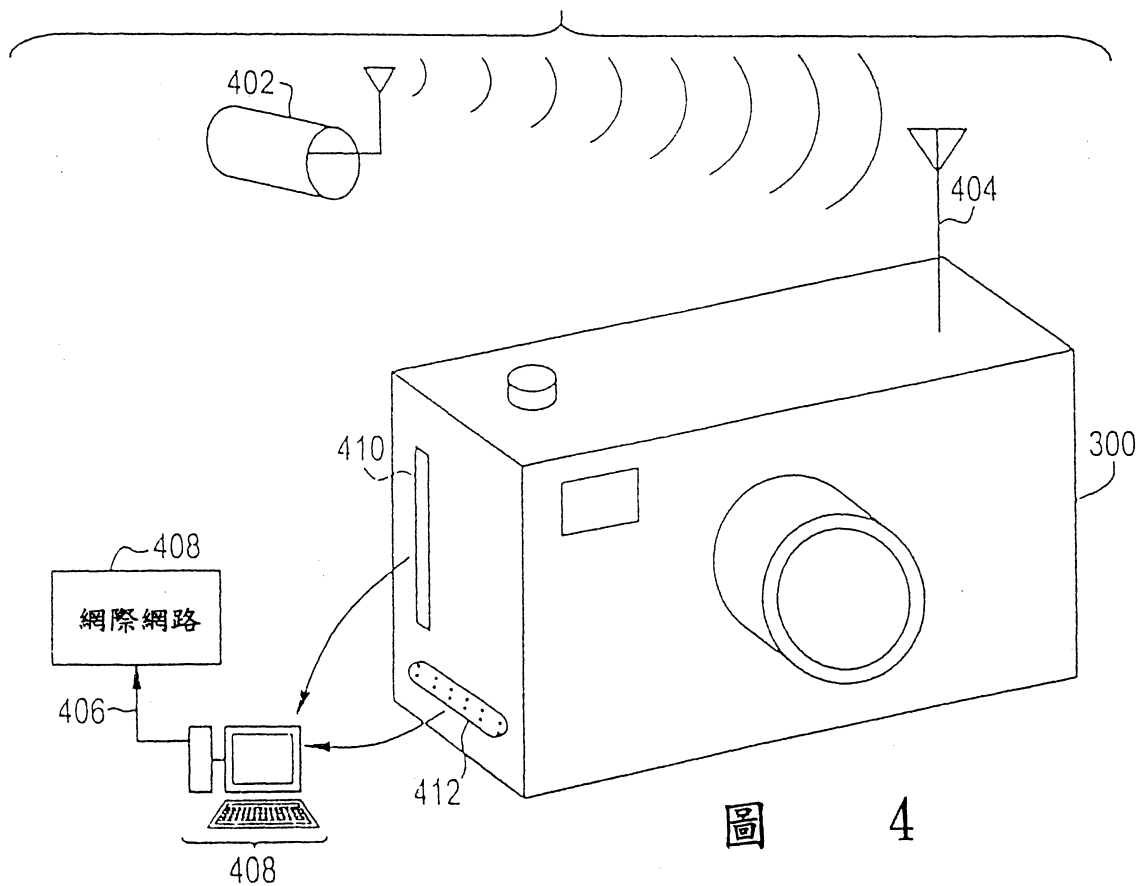


圖 4

圖式

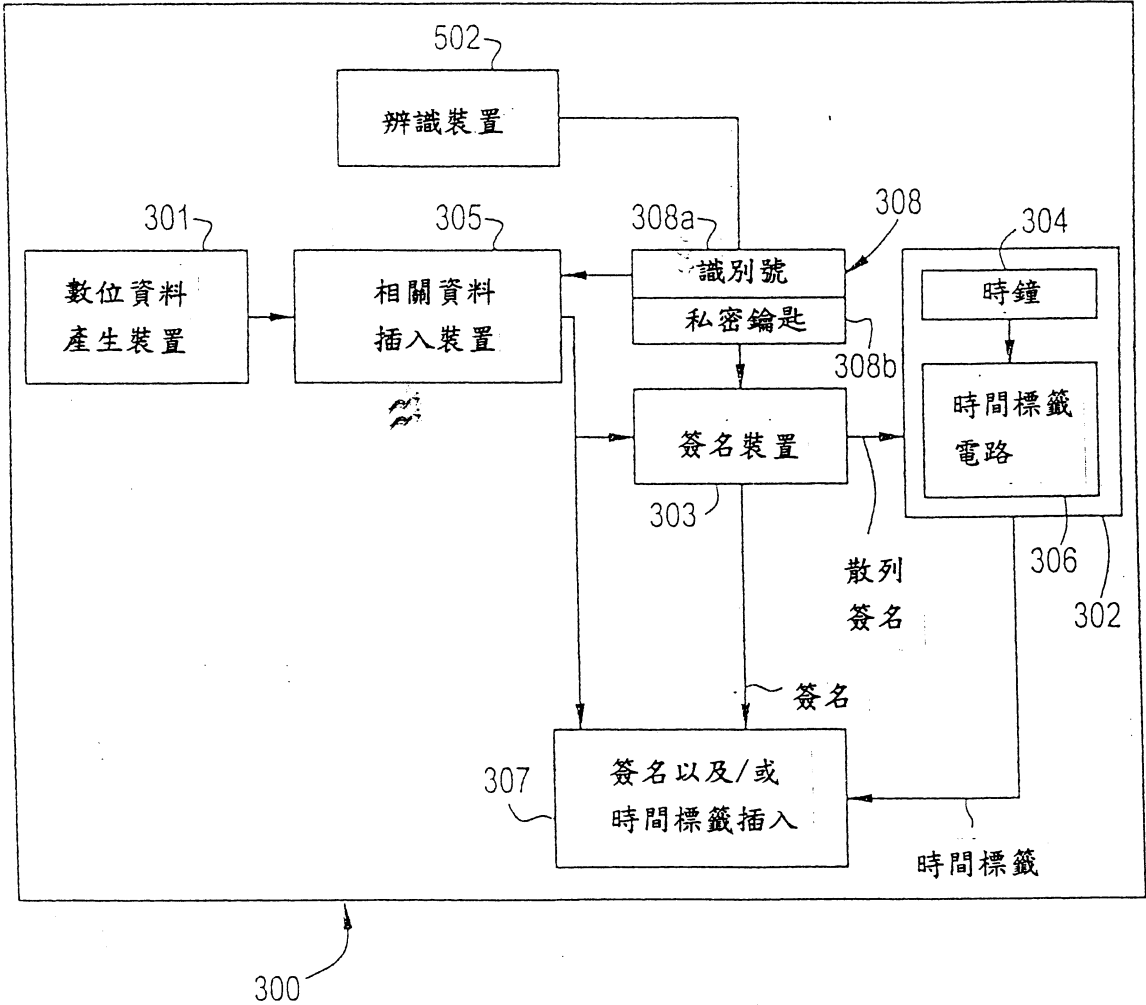


圖 5

圖式簡單說明

元 件 符 號 說 明

100	數位影像
102	影像畫素
104	位元
106	最高有效位元(MSB)
108	最低有效位元(LSB)
110	最高有效位元平面
112	最低有效位元平面
114	頻率領域
116	高頻率元件
118	低頻率元件
120	LSB平面之部分
122	相關資料
122a, 122b	區域
124	樣本(行)
300	攝影機或影像產生裝置
301	數位資料產生裝置
302	半導體晶片
303	簽署裝置
304	防搗毀時鐘
305	相關資料插入裝置
306	防搗毀時間標籤電路
307	資料插入裝置
308	記憶體



圖式簡單說明

400	影像產生裝置
402	外部資源
404	接收裝置
406	網際網路連接
408	個人電腦及網際網路
410	記憶卡插槽
412	有線裝置
502	辨識裝置



六、申請專利範圍

1. 一種用以插入數位簽名於包括位元之數位資料中之方法，包括下列步驟：

指定用以接收數位簽名之數位資料之預定位元；

簽署除造成數位簽名之預定位元以外之數位資料；以及

插入數位簽名於數位資料之預定位元，以便做為隨後數位資料之驗證。

2. 如申請專利範圍第1項之方法，其中簽名步驟包括：

應用一單方向散列功能施於排除了造成散列之預定位元之數位資料上。

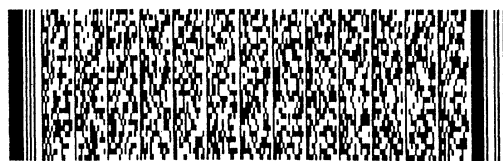
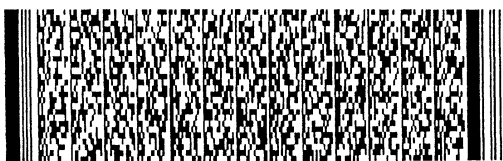
3. 如申請專利範圍第1項之方法，其中數位資料是從由影像資料、連續影像資料、以及聲音資料組成之群組中選擇出來。

4. 如申請專利範圍第1項之方法，進一步包括的步驟為插入相關資料於先於簽名步驟之數位資料中。

5. 如申請專利範圍第4項之方法，其中相關資料插入於除預定位元以外之數位資料位元中。

6. 如申請專利範圍第4項之方法，其中數位資料包括多個樣本，每個樣本經由多個位元所定義，從最高有效位元到最低有效位元，所有定義多個樣本之最低有效位元包括一最低有效位元平面，其中預定位元包括至少一部分最低有效位元平面。

7. 如申請專利範圍第6項之方法，其中相關資料插入於最低有效位元平面中之至少一部分剩餘最低有效位元。



六、申請專利範圍

8. 如申請專利範圍第4項之方法，其中數位資料包括多個樣本，每個樣本經由多個位元所定義，進一步包括轉變多個位元為具有至少第一與第二特徵成份之另一種形式之步驟，其中預定位元包括第一特徵成份。

9. 如申請專利範圍第6或8項之方法，其中數位資料為影像，而每個樣本為影像畫素。

10. 如申請專利範圍第6或8項之方法，其中數位資料為連續影像，而每個樣本為空間性暫時樣本。

11. 如申請專利範圍第6或8項之方法，其中數位資料為聲音，而每個樣本為時間樣本。

12. 如申請專利範圍第8項之方法，其中相關資料插入於至少一部分第二特徵成份。

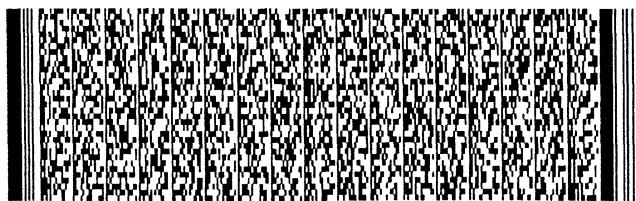
13. 如申請專利範圍第12項之方法，其中另一種表現形式為具有高和低頻率成份之頻率領域表現形式，其中第一特徵成份為部分高頻率成份，而第二特徵成份為剩餘高頻率成份以及低頻率成份。

14. 如申請專利範圍第4項之方法，其中至少一部分相關資料包括辨識用來解譯數位簽名之公用鑰匙之資料。

15. 如申請專利範圍第4項之方法，其中相關資料包括辨識數位資料來源之資料。

16. 如申請專利範圍第4項之方法，其中相關資料包括辨識數位資料擁有者身份之資料。

17. 如申請專利範圍第16項之方法，其中數位資料為影像，並且相關資料包括辨識影像照相者之資料。



六、申請專利範圍

18. 如申請專利範圍第4項之方法，其中加密編譯部分相關資料，而剩餘部分相關資料則不加密編譯。

19. 如申請專利範圍第4項之方法，其中相關資料至少包括兩個區域。

20. 如申請專利範圍第19項之方法，其中至少一區域包括辨識用來解譯數位簽名之公用鑰匙之資料。

21. 如申請專利範圍第20項之方法，其中至少另一區域包括辨識公用鑰匙擁有者之資料。

22. 如申請專利範圍第4項之方法，進一步包括之步驟為從外部資源接收相關資料。

23. 如申請專利範圍第22項之方法，其中外部資源為全球衛星定位系統。

24. 如申請專利範圍第1項之方法，其中使用造成壓縮檔案之壓縮標準壓縮數位資料，而其中進一步包括下列步驟：

在簽名步驟之前創造一解壓縮檔案；簽署造成數位簽名之解壓縮檔案；以及

插入數位簽名於壓縮檔案之檔案頭中，以取代插入數位簽名於數位資料中。

25. 如申請專利範圍第4項之方法，其中使用造成壓縮檔案之壓縮標準壓縮數位資料，而其中進一步包括下列步驟：

在簽名步驟之前創造一解壓縮檔案；

插入相關資料於解壓縮檔案中；



六、申請專利範圍

簽署造成數位簽名之解壓縮檔案；以及

插入數位簽名與相關資料於壓縮檔案之檔案頭中，
以取代插入數位簽名與相關資料於數位資料中。

26. 如申請專利範圍第24或25項之方法，其中數位資料為影像且壓縮標準為JPEG。

27. 如申請專利範圍第24或25項之方法，其中數位資料為連續影像且壓縮標準為MPEG。

28. 如申請專利範圍第4項之方法，其中數位資料包括多個樣本，每個樣本經由多個位元所定義，從最高有效位元到最低有效位元，所有定義多個樣本之最低有效位元包括一最低有效位元平面，其中此方法進一步包括下列步驟：

忽略數位資料中之最低有效位元平面；

在簽名步驟之前，連接相關資料至具有忽略的最低有效位元平面之數位資料；

執行簽名步驟於具有造成數位簽名之連結的相關資料之數位資料；

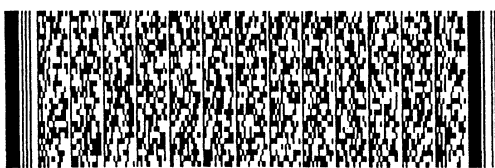
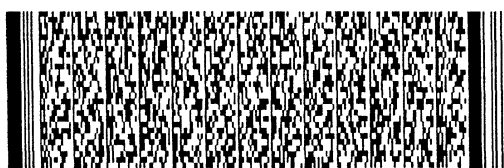
其中預定位元包括至少一部分最低有效位元平面，且相關資料插入於至少一部分最低有效位元平面中之剩餘最低有效位元。

29. 如申請專利範圍第1項之方法，進一步包括下列步驟：

提供辨識創造數位資料時間之時間資料；

連接散列與時間資料；

應用單方向散列功能於連接散列和造成第二次散列



六、申請專利範圍

之時間資料；以及

加密編譯第二散列取代第一散列，以造成包含數位簽名之時間標籤，其中數位資料與時間資料隨後驗證之。

30. 如申請專利範圍第29項之方法，進一步包括下列步驟：

傳送散列與簽名至第三者以提供、連接、與加密編譯步驟，以及

在插入步驟之前從第三者接收時間標籤。

31. 如申請專利範圍第30項之方法，其中可信賴的第三者存在於一網際網路位址上，且傳送與接收步驟經由網際網路完成。

32. 如申請專利範圍第29項之方法，其中經由具有防搗毀時鐘與防搗毀時間標籤之半導體晶片，電路提供時間標籤，其中時鐘輸出時間資料與數位簽名一起經由電路簽署以輸出時間標籤。

33. 如申請專利範圍第4項之方法，進一步包括下列步驟：

根據創造數位資料裝置之至少一位使用者儲存識別號於記憶體中；

辨認其識別號儲存於記憶體中之裝置使用者；

根據辨認出的使用者從將要插入作為相關資料之記憶體輸出識別號。

34. 如申請專利範圍第33項之方法，進一步包括之步驟為根據每個使用者儲存私密鑰匙以簽署記憶體中之數位資



六、申請專利範圍

料，並使用私密鑰匙以簽署數位資料。

35. 如申請專利範圍第33項之方法，其中辨認步驟經由指紋辨認系統完成。

36. 如申請專利範圍第33項之方法，其中識別號為辨識出的使用者名字。

37. 一種用以驗證在數位資料預定位元中具有嵌入式數位簽名之數位資料之方法，該方法包括下列步驟：

從預定位元取出數位簽名；

從造成第一散列之數位資料解譯數位簽名；

應用由數位資料編碼器所使用之單方向散列功能於除了造成第二散列之預定位元以外之數位資料；以及

比較第一散列與第二散列，其中假如第一散列與第二散列相符時，數位資料則為已驗證。

38. 如申請專利範圍第37項之方法，其中數位資料從一包含影像資料、連續影像資料、與聲音資料之群組中選擇出來。

39. 如申請專利範圍第37項之方法，其中數位資料進一步包括插入於已知數位資料位元中之相關資料，其中此方法驗證了相關資料以及數位資料。

40. 如申請專利範圍第39項之方法，其中相關資料插入於排除預定位元之數位資料位元中。

41. 如申請專利範圍第39項之方法，其中使用造成壓縮檔案之壓縮標準壓縮數位資料，並且其中數位簽名與相關資料包含於壓縮檔案頭之中，其中此方法進一步包括下列



六、申請專利範圍

步驟：

解壓縮壓縮檔；以及

在取出步驟之前，分別從檔案頭將簽名與相關資料替代至預定位元與已知位元中。

42. 一種用以插入數位簽名於數位資料中之編碼器，數位資料包括位元，編碼器包括：

用以指定數位資料預定位元之裝置，以接收數位簽名；

用以簽署除造成數位簽名之預定位元以外之數位資料之裝置，以及

用以插入數位簽名於數位資料之預定位元之裝置，以隨後驗證數位資料。

43. 如申請專利範圍第42項之編碼器，其中用以簽名之裝置包括：

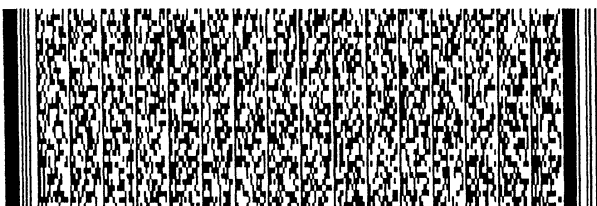
用以應用單方向散列功能於排除了散列之預定位元之數位資料上之裝置；以及

加密編譯散列。

44. 如申請專利範圍第42項之編碼器，其中數位資料從一包含影像資料、連續影像資料、與聲音資料之群組中選擇出來。

45. 如申請專利範圍第42項之編碼器，進一步包括在簽署數位資料之前，用以插入相關資料於數位資料中之裝置，如此一來編碼器驗證相關資料以及數位資料。

46. 如申請專利範圍第45項之編碼器，其中相關資料插



六、申請專利範圍

入於排除了預定位元之數位資料位元中。

47. 如申請專利範圍第45項之編碼器，其中數位資料包括多個樣本，樣本經由從最高有效位元到最低有效位元之多個位元所定義，所有最低有效位元定義多個樣本包括了一最低有效位元平面，其中預定位元包括至少一部分最低有效位元平面。

48. 如申請專利範圍第47項之編碼器，其中相關資料插入於至少一部分最低有效位元平面中之剩餘最低有效位元。

49. 如申請專利範圍第45項之編碼器，其中數位資料為包括多個樣本之影像，每個樣本經由多個位元所定義，進一步包括用以轉變多個位元為另一種具有至少第一和第二特徵成份之表現方式之裝置，其中預定位元包括第一特徵成份。

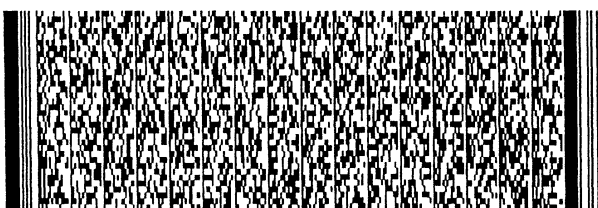
50. 如申請專利範圍第47或49項之編碼器，其中數位資料為影像，且每個樣本為影像畫素。

51. 如申請專利範圍第47或49項之編碼器，其中數位資料為連續影像，且每個樣本為空間性暫時樣本。

52. 如申請專利範圍第47或49項之編碼器，其中數位資料為聲音，且每個樣本為時間樣本。

53. 如申請專利範圍第49項之編碼器，其中相關資料插入於至少一部分第二特徵成份。

54. 如申請專利範圍第53項之編碼器，其中另一種表現方式具有高和低頻率成份，其中第一特徵成份為一部分高



六、申請專利範圍

頻率成份，第二特徵成份為剩餘高頻率成份和低頻率成份。

55. 如申請專利範圍第45項之編碼器，其中至少一部分相關資料包括辨識公用鑰匙之資料，以用來解譯數位簽名。

56. 如申請專利範圍第45項之編碼器，其中相關資料包括辨識數位資料來源之資料。

57. 如申請專利範圍第45項之編碼器，其中相關資料包括辨識數位資料使用者身份之資料。

58. 如申請專利範圍第57項之編碼器，其中數位資料為影像，相關資料包括辨識影像照相者之資料。

59. 如申請專利範圍第45項之編碼器，其中部分相關資料加密編譯，剩餘的部分相關資料則不加密編譯。

60. 如申請專利範圍第45項之編碼器，其中相關資料包括至少兩個區域。

61. 如申請專利範圍第60項之編碼器，其中至少一區域包括辨識公用鑰匙之資料，以用來解譯數位簽名。

62. 如申請專利範圍第61項之編碼器，其中至少另一區域包括辨識公用鑰匙擁有者之資料。

63. 如申請專利範圍第57項之編碼器，進一步包括用以從外部資源接收相關資料之裝置。

64. 如申請專利範圍第63項之編碼器，其中外部資源為全球衛星定位系統。

65. 如申請專利範圍第42項之編碼器，其中使用造成壓



六、申請專利範圍

縮檔案之壓縮標準壓縮數位資料，其中編碼器進一步包括：

用以在簽署數位資料之前創造解壓縮檔案之裝置；
用以簽署造成數位簽名之解壓縮檔案之裝置；以及
用以插入數位簽名於壓縮檔之檔案頭，以取代插入於數位資料中之裝置。

66. 如申請專利範圍第45項之編碼器，其中使用造成壓縮檔案之壓縮標準壓縮數位資料，其中編碼器進一步包括：

用以在簽署數位資料之前創造解壓縮檔案之裝置；
用以插入相關資料於解壓縮檔案中之裝置；
使用插入的相關資料，用以簽署解壓縮檔案之裝置，其中插入的相關資料造成數位簽名；以及

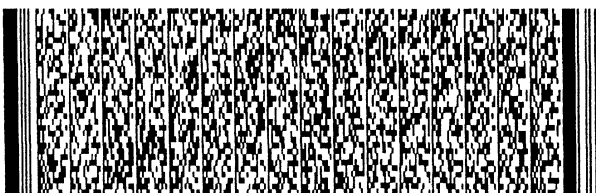
用以插入數位簽名與相關資料於壓縮檔之檔案頭，以取代插入於數位資料中之裝置。

67. 如申請專利範圍第65或66項之編碼器，其中數位資料為影像，壓縮標準為JPEG。

68. 如申請專利範圍第65或66項之編碼器，其中數位資料為連續影像，壓縮標準為MPEG。

69. 如申請專利範圍第45項之編碼器，其中數位資料包括多個樣本，樣本經由從最高有效位元到最低有效位元之多個位元所定義，所有最低有效位元定義多個樣本包括了一最低有效位元平面，其中編碼器進一步包括：

用以忽略至少一部分數位資料中之最低有效位元平



六、申請專利範圍

面之裝置；

在簽署數位資料之前，用以連接相關資料至具有忽略的最低有效位元平面之數位資料之裝置；

用以簽署具有造成數位簽名之連接的相關資料之數位資料之裝置；

其中預定位元包括至少一部分最低有效位元平面，且相關資料插入於至少一部分最低有效位元平面中之剩餘最低有效位元。

70. 如申請專利範圍第45項之編碼器，進一步包括：

用以提供辨識創造數位資料時間資料之裝置；

用以連接散列與時間資料之裝置；

用以應用單方向散列功能於連接的散列，與造成第二散列之時間資料；以及

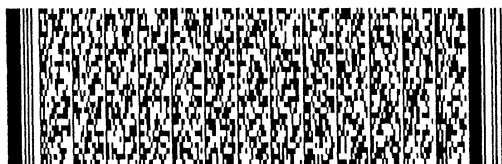
用以加密編譯第二散列以取代第一散列之裝置，以造成包含數位簽名之時間標籤，其中數位資料與時間資料隨後驗證之。

71. 如申請專利範圍第70項之編碼器，進一步包括：

用以傳送散列至一第三者，以提供時間標籤以及連接散列與時間標籤之裝置；以及

在加密編譯之前，用以從該第三者接收第二散列之裝置。

72. 如申請專利範圍第71項之編碼器，其中可信賴的第三者存在於一網際網路位址上，用以傳送和接收之裝置為可存取網際網路和接收傳送的第二散列之電腦。



六、申請專利範圍

73. 如申請專利範圍第70項之編碼器，進一步包括具有防搗毀時鐘與防搗毀時間標籤電路之半導體晶片，其中時鐘輸出時間資料與數位簽名一起經由電路簽署以輸出時間標籤。

74. 如申請專利範圍第45項之編碼器，進一步包括：

用以儲存對應至少一創造數位資料裝置使用者之識別號之記憶體；

用以辨識其識別號儲存於記憶體中之裝置使用者之辨識裝置；以及

用以輸出對應來自記憶體之辨識的使用者，以插入作為相關資料之識別號之輸出裝置。

75. 如申請專利範圍第74項之編碼器，其中用以簽署數位簽名之私密鑰匙也儲存於對應每個使用者之記憶體中，其中識別號插入以作為相關資料，且私密鑰匙用來簽署數位資料。

76. 如申請專利範圍第74項之編碼器，其中辨識裝置為指紋辨認系統。

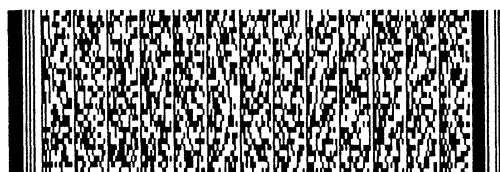
77. 如申請專利範圍第76項之編碼器，其中識別號為辨識的使用者之名字。

78. 一種用以驗證具有於數位資料預定位元中之嵌入式數位簽名之數位資料之解碼器，解碼器包括：

用以從預定位元取出數位簽名之裝置；

用以從造成第一散列之數位資料解譯簽名之裝置；

用以施加單方向散列功能於除造成第二散列之預定



六、申請專利範圍

位元之數位資料以外之裝置；以及

用以比較第一散列與第二散列之裝置，其中假如第一散列與第二散列相符時，數位資料則為已驗證。

79. 如申請專利範圍第78項之解碼器，其中數位資料從一包含影像資料、連續影像資料、與聲音資料之群組中選擇出來。

80. 如申請專利範圍第78項之解碼器，其中數位資料進一步包括插入於數位資料已知位元之相關資料，其中解碼器驗證相關資料以及數位資料。

81. 如申請專利範圍第80項之解碼器，其中相關資料插入於排除了預定位元之數位資料位元中。

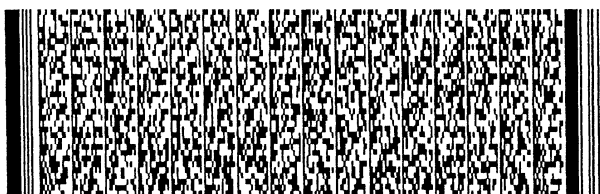
82. 如申請專利範圍第80項之解碼器，其中使用造成壓縮檔案之壓縮標準壓縮數位資料，且其中數位簽名包含於壓縮檔案之檔案頭中，其中編碼器進一步包括：

用以解壓縮壓縮檔案之裝置；以及

在從預定位元取出數位簽名之前，用以從檔案頭取代簽名為預定位元之裝置。

83. 如申請專利範圍第80項之解碼器，其中使用造成壓縮檔案之壓縮標準壓縮數位資料，且其中數位簽名與相關資料包含於壓縮檔案之檔案頭中，其中編碼器進一步包括：

用以解壓縮壓縮檔案之裝置；以及



六、申請專利範圍

在從預定位元取出數位簽名之前，用以分別從檔案頭取代簽名與相關資料為預定位元與已知位元之裝置。

84. 一種用以插入資料於數位資料中以便隨後驗證數位資料之方法，該方法包括下列步驟：

從外部資源接收資料；

插入資料於數位資料中；以及

驗證數位資料。

85. 如申請專利範圍第84項之方法，其中外部資源為射頻傳送。

86. 如申請專利範圍第84項之方法，其中外部資源為網際網路連接。

87. 如申請專利範圍第84項之方法，其中插入的資料用來驗證與數位資料一起的資訊。

88. 一種用以插入資料於數位資料中以便隨後驗證數位資料之裝置，該裝置包括：

用以從外部資源接收資料之裝置；

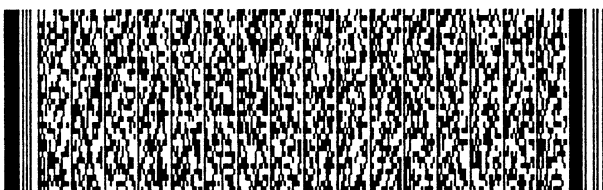
用以插入資料於數位影像中之裝置；以及

用以驗證數位資料之裝置。

89. 如申請專利範圍第88項之裝置，其中外部資源為射頻傳送，用以接收資料之裝置包括天線。

90. 如申請專利範圍第88項之裝置，其中外部資源為網際網路連接用以接收資料之裝置包括可存取網際網路和接收資料之電腦。

91. 如申請專利範圍第88項之裝置，其中插入的資料用



六、申請專利範圍

來驗證與數位資料一起的資訊。

92. 一種用以插入時間資料於數位資料中以便隨後驗證時間資料與數位資料之方法，該方法包括下列步驟：

提供一具有防搗毀時鐘與時間標籤電路之半導體晶片；

從時鐘輸出數位簽名與時間資料至時間標籤電路；
簽署時間資料與造成時間標籤之數位簽名；以及
驗證數位資料與時間資料。

93. 一種用以插入時間資料於數位資料中以便隨後驗證時間資料與數位資料之裝置，該裝置包括：

具有防搗毀時鐘與時間標籤電路之半導體晶片；

用以從時鐘輸出數位簽名與時間資料至時間標籤電路之裝置；以及

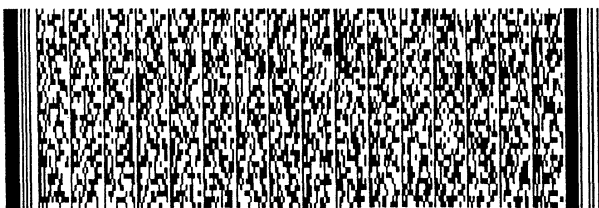
用以簽署時間資料與造成時間標籤之數位簽名之裝置。

94. 如申請專利範圍第88或93項之裝置，其中該裝置為數位影像產生裝置，且數位資料代表影像。

95. 如申請專利範圍第94項之裝置，其中影像產生裝置從一包含數位攝影機、數位連續影像攝影機、與數位掃描器之群組中選擇出來。

96. 一種用以插入資料於數位資料中之方法，該方法包括：

儲存對應於用來產生數位資料之裝置之至少一使用者之識別號；



六、申請專利範圍

辨識該裝置之使用者，其中該使用者之識別號儲存於記憶體中；

自該記憶體輸出對應於經辨識使用者之該識別號；
以及

插入對應識別號之資料於數位資料中。

97. 如申請專利範圍第96項之方法，其中插入的資料用來驗證數位資料。

98. 如申請專利範圍第96項之方法，其中插入的資料用來驗證與數位資料一起的資訊。

99. 如申請專利範圍第96項之方法，其中識別號為辨識的使用者之名字。

100. 一種用以插入資料於數位資料中之裝置，該裝置包括：

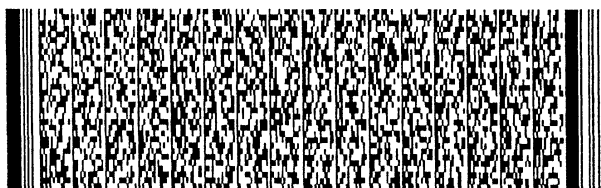
用以儲存對應於該裝置之至少一使用者之識別號之記憶體；

用以辨識該裝置之使用者之辨識裝置，其中該識別號儲存於該記憶體中；

用以自該記憶體輸出對應於經辨識使用者之識別號之裝置；以及

用以對應識別號插入資料於數位資料中之裝置。

101. 如申請專利範圍第100項之裝置，其中用以簽署數位資料之私密鑰匙也儲存於對應每個使用者之記憶體中，其中識別號插入於數位資料中，且私密鑰匙用來簽署隨後之數位資料。



六、申請專利範圍

102. 如申請專利範圍第100項之裝置，其中辨識裝置為指紋辨認系統。

103. 如申請專利範圍第100項之裝置，其中該裝置為數位影像產生裝置，且數位資料代表影像。

104. 如申請專利範圍第100項之裝置，其中影像產生裝置從一包含數位攝影機、數位連續影像攝影機、與數位掃描器之群組中選擇出來。

