發明專利說明書 200411596

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※申請案號：091137276　※IPC分類：G09C 5/00

※申請日期：91-12-25

壹、發明名稱

（中文）電子文件及其列印驗證方法

（英文）Electrical document and the verifying method for the electrical document

貳、發明人（共 3 人）

發明人 1 （如發明人超過一人，請填**說明書發明人續頁**）

姓名：（中文）吳彥興

（英文）Yen-Hsing Wu

住居所地址：（中文）台北市大安區光復南路626號5樓

（英文）5F, 626, Kuang-Fu S. Road, Taipei, Taiwan

國籍：（中文）中華民國　（英文）

參、申請人（共 1 人）

申請人 1 （如發明人超過一人，請填**說明書申請人續頁**）

姓名或名稱：（中文）財團法人工業技術研究院

（英文）Industrial Technology Research Institute

住居所或營業所地址：（中文）新竹縣竹東鎮中興路4段195號

（英文）195, Sec. 4, Chung Hsing Rd. Chutung, Hsinchu, Taiwan

國籍：（中文）中華民國　（英文）

代表人：（中文）翁政義

（英文）

V 續發明人或申請人續頁 （發明人或申請人欄位不敷使用時，請註記並使用續頁）

說明書發明人續頁

發明人 2

姓名：（中文）吳 東 霖

（英文）Tung-Lin Wu

住居所地址：（中文） 桃園縣龜山鄉民安街 64 巷 17 弄 25 號

（英文） 25, Alley 17, Lane 64, Minan St. Gwei Shan, Taoyuan, Taiwan

國籍：（中文） 中 華 民 國 （英文）

發明人 3

姓名：（中文） 林 志 杰

（英文） Lin, Chih-Chieh

住居所地址：（中文） 台北市北投區洲美街 219 號

（英文） 219, Joumei St. Beitou Chiu, Taipei, Taiwan

國籍：（中文） 中 華 民 國 （英文）

發明人 4

姓名：（中文）

（英文）

住居所地址：（中文）

（英文）

國籍：（中文） （英文）

發明人 5

姓名：（中文）

（英文）

住居所地址：（中文）

（英文）

國籍：（中文） （英文）

捌、聲明事項

☐ **本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：** _____

☐ **本案已向下列國家（地區）申請專利，申請日期及案號資料如下：**

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1. _____
2. _____
3. _____

☐ **主張專利法第二十四條第一項優先權：**

【格式請依：受理國家（地區）；日期；案號　順序註記】

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

☐ **主張專利法第二十五條之一第一項優先權：**

【格式請依：申請日；申請案號　順序註記】

1. _____
2. _____
3. _____

☐ **主張專利法第二十六條微生物：**

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1. _____
2. _____
3. _____

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1. _____
2. _____
3. _____

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

【發明所屬之技術領域】

本發明係關於一種電子文件及其列印驗證方法，尤指一種可辨識列印出的文件資料是否為具有法律效力之原本，而杜絕偽造可能性之驗證方法。

【先前技術】

在電子化政府的政策目標下，電子文件的傳遞、列印為相當重要的部分，一般的傳遞方式可以透過數位化多位元加密方式，將原本數位內容之文件經由不同長度位元作編碼加密後，透過網際網路傳遞至另一目標端，當目標端經過解碼解密後，還原成原本的數位文件內容。

雖然文件電子化可大幅提昇流程的作業速度，然而某些特定的文件仍有其列印必要性。一般列印的方式係可透過噴墨、雷射印表機等做為列印機構，但在列印後，卻無法辨認該列印出的電子文件與原本是否相同，更甚者，若有刻意偽造電子文件紙本列印，依據目前技術亦無法指認其為偽造文件。此點也是導致電子公文化或其它必須經過認證程序的電子文件無法普及之一重大因素。

在美國第 5,606,609 發明專利案中大致上已揭露了電子文件加密與解密的驗證方式，但在列印的部分，僅是說明經過驗證的文件可以透過印表機列印出，並未說明如何辨認其列印後文件為單一正本，而關於列印的細節並未加以詳述。

再者，另一美國專利案第 5,974,548 號係提出一列印加密方法，用以追蹤電子文件於列印後的傳遞流程，但卻並未提出如何辨認偽造文件及驗證列印出的文件。

請參考第四圖所示，為另一美國專利案第 6,389,151 號所提出的加密方式，其根據不同的數位資料型態，例如圖像、數位資料、電腦圖案等，採用不同的模板和佈局的方法來藏入欲加入的數位浮水印資料，最後輸出至列印機器，以得到加密後的文件。而對於列印出來的文件，其驗證方式是根據不同資料型態的文件，採取不同的讀入方式，但並未具有其詳細的實施流程，且同樣未說明如何辨認其列印後文件為「單一正本」。

【發明內容】

有鑑於前述習用方式均無法辨識列印出的文件係屬原本，造成電子文件（如公家機關公文）無法廣泛採用的缺點，故本發明之主要目的係在提供一種電子文件及其列印驗證方法，可用以檢驗列印出的文件是否為具有法律效力的原本資料。

為達成前述目的，本發明之驗證方式係針對列印出來的電子文件賦予一加密手段，並於列印之際同步傳送此加密資料予一驗證資料儲存單位交其儲存，當前述列印出來之紙本資料於其餘場合使用時，由使用單位連線取得該驗證資料儲存單位所存之加密資料，以核對文件是否與原本相符。

前述賦予電子文件之加密手段，其具體可行方式係包含有以下數種：

建立文件辨識序號，係由發出電子文件的發文單位於產生文件之際，即將一文件辨識序號賦予該電子文件。

賦予文件印表機序號，當收執端取得一來自發文單位之電子文件而進行列印時，利用各台印表機出廠序號互不重覆之特點，可將執行列印工作之印表機的序號列印於該電子文件上。

賦予文件列印參數，係將列印文件同時，將印表機之列印韌體所記錄下的狀況參數列印出來，如列印噴墨頭之移動次數、啟動的噴墨噴孔數、使用的紙張編碼、及當時列印時，印表機內部更新的總頁數等。

前述三種加密手段係可獨立施加於電子文件上，或是採組合方式實施。

又，對應前述加密手段，本發明之解密手段係為：

該電子文件成功列印後，其所賦予的各項加密資料係傳送至一驗證資料儲存單位儲存；

連線至前述驗證資料儲存單位並讀取該電子文件所賦予的各項加密資料；

比對該電子文件上之各加密資料，若完全正確則證明該電子文件為原本。

【實施方式】

請參閱第一圖所示，為本發明之驗證方法示意圖，當一發文單位（１０）產生一電子文件時，係同時將一組代表該電子文件之序號傳送予一驗證資料儲存單位（２０），而於收文單位（３０）取得此份電子文件且進一步列印時，於列印當下亦將列印狀態資料交付該驗證資料儲存單位（２０），故一旦此份列印文件欲於其它地方使用時，使用者可藉由前述驗證資料儲存單位（２０）當中的資訊判斷該列印文件是否為原本。

為具體說明本發明之實施方式，以公家機關為例應用在公文電子化的實施，則前述的發文單位（１０）可由各級行政單位組成，而驗證資料儲存單位（２０）則為全國性的單一機構，收文單位（３０）除涵括有行政單位之外，亦可包含一般民眾。

當一份電子文件由發文單位（１０）建立產生時，係可同時賦予一組文件序號，此組文件序號因為由公家機構編制，故可加以掌控而避免序號重覆。

於電子文件利用網路傳遞予收文單位（１０）後，無論其對象是一公家單位或是一般民眾，若此份電子文件必須加以列印使用，則於列印時將對此紙本文件進行加密程序。其加密方式包括有：

１．利用出廠印表機之序號：印表機在出廠時，在機器端內部唯讀記憶體中，可以加入印表機出廠序號。此序號可採用現有一般 802.3 乙太網路卡的 MAC 編碼位址，由網路卡晶片廠商向網路管理中心取得廠商編號，

廠商再依據網路晶片卡製造量做編號，最後二者編號合併後，即可成為 MAC 編碼位址。相同的，印表機廠商亦可成立一全球化的印表機序號管理中心，此管理中心針對不同的印表機廠商作編號，印表機廠商再針對印表機出廠時，對印表機做出廠編號，此二者編號合併後，及可以成為印表機出廠序號。此印表機出廠序號具有全世界唯一性，換句話說，若經過全球化的印表機序號管理中心管理的廠商，是不會產生出二組相同的印表機序號。

2．利用列印狀態參數：印表機於列印時，在列印時的列印韌體（Firmware）可以記錄下當時列印的狀況，列印狀況可包含列印噴墨頭前後移動次數、啟動的噴墨噴孔數、使用的紙張編碼、及當時列印的頁數。所謂當時列印的頁數係指印表機從出廠後所列印成功的總累計頁數，總頁數在同一台印表機中，一般狀況係為單一，絕無可能產生二組相同的列印總頁數。

請參考第二圖所示，前述施加於該電子文件上的加密資料，係直接列印於電子文件上，其流程如圖所示：

當收文單位（３０）的一方開始列印文件時，印表機韌體控制單元（４０）係從韌體控制參數（４１）中取出相對應的參數（例如列印總頁數、列印噴頭數、解析度等）經由韌體控制單元（４０），以 IEEE 1284 或 USB 纜線傳遞回傳至列印驅動程式（Printer Driver），由列印驅動程式決定加密資料是用一維條碼、二維條碼

或浮水印的方式列印。最後，此份電子文件將做列印色彩與半色調轉換後並將其以印表機列印語言以編碼，且加入前述文件序號、印表機序號及韌體控制參數等，經由資料排線將列印資訊傳遞至印表機韌體控制單元（４０），利用印表機機構進行解碼列印而成為一份列印加密文件。列印成功後，列印驅動程式係將此份文件相關的編碼資訊傳遞回驗證資料儲存單位（２０）。

請參閱第三、四圖所示，當持有前述列印加密文件的使用者欲應用該份文件時，收取文件的單位係檢驗其是否為原本。收文單位係根據文件上列印的加密資訊判斷應由何種方式掃瞄讀取，同時連線至驗證資料儲存單位（２０）取得當初該份文件於列印時所賦予的加密資訊為何，若全部比對無誤後即證明該份紙本文件係為原發文單位（１０）所送出的原本而非偽造。

綜上所述，本發明之電子文件及其列印驗證方法，係可驗證電子文件於列印使用之際係為原本無誤，且可有效檢測出刻意偽造非法情事，相較於習用諸多驗證方式，更見其進步性而實際應用性，係符合發明專利之申請要件，爰依法具文提出申請。

【圖式簡單說明】

（一）圖式部份：

第一圖：係本發明一較佳實施例之示意圖。

第二圖：係本發明列印加密一較佳實施例之示意圖。

第三圖：係本發明解密示意圖。

第四圖：係一習用文件之加密步驟示意圖。

（二）元件代表符號：

（１０）發文單位

（２０）驗證資料儲存單位

（３０）收文單位

（４０）印表機韌體控制單元

（４１）韌體控制參數

肆、中文發明摘要

本發明係關於一種電子文件及其列印驗證方法，係於電子文件列印之際係賦予加密資料，並同步傳送此加密資料予一驗證資料儲存單位交其儲存，當該電子文件列出後為其它單位使用時，可連線取得該驗證資料儲存單位所存之加密資料，以核對該文件是否與原本相符無訛，其中該加密資料係可包括有：文件辨識序號、印表機序號或列印狀態參數等數種。

伍、英文發明摘要

The present invention is related to an electrical document and a verifying method for the electrical document. When a hard copy is being printed from the electronic document, encryption information is applied on the printed document and also simultaneously transmitted to an information storage center. Thereby, when the printed document is applied or used at other occasions, any document receiving unit is able to verify whether the printed document is identical to the electrical document by checking the encryption information stored in the information storage center. The encryption information may be chosen from the serial number of the electrical document, the serial number or the printing parameters of a printer, which executes the electrical document printing job.

拾、申請專利範圍

1．一種電子文件之列印驗證方法，係對列印出來之電子文件賦予加密資料，並於列印之際同步傳送該加密資料予一驗證資料儲存單位儲存，於該列印出之電子文件於應用時，可由使用者連線取得該驗證資料儲存單位所存之加密資料，而核對文件是否為原本。

2．如申請專利範圍第1項所述電子文件之列印驗證方法，該加密資料係為一文件辨識序號，由發出該電子文件之發文單位所賦予。

3．如申請專利範圍第1項所述電子文件之列印驗證方法，該加密資料係為執行列印工作之印表機的序號。

4．如申請專利範圍第1項所述電子文件之列印驗證方法，該加密資料係為列印狀態參數。

5．如申請專利範圍第4項所述電子文件之列印驗證方法，該列印狀態參數包含有列印驅動程式因本次列印文件產生的列印工作序號、列印噴墨頭之移動次數、啟動的噴墨噴孔數、使用的紙張編碼、及當時列印之總頁數。

6．如申請專利範圍第2、3、4或5項所述電子文件之列印驗證方法，前述加密資料係以一維條碼方式列印。

7．如申請專利範圍第2、3、4或5項所述電子文件之列印驗證方法，前述加密資料係以二維條碼方式

列印。

8．如申請專利範圍第2、3、4或5項所述電子文件之列印驗證方法，前述加密資料係以浮水印方式列印。

9．一種列印有加密資料之電子文件，其中該加密資料係可與一驗證資料儲存單位之加密資訊相互比對，以驗證該列印出之電子文件係為原本。

10．如申請專利範圍第9項所述列印有加密資料之電子文件，該加密資料係為一文件辨識序號，由發出該電子文件之發文單位所賦予。

11．如申請專利範圍第9項所述列印有加密資料之電子文件，該加密資料係為執行列印工作之印表機的序號。

12．如申請專利範圍第9項所述列印有加密資料之電子文件，該加密資料係為列印狀態參數。

13．如申請專利範圍第12項所述列印有加密資料之電子文件，前述列印狀態參數包含有列印驅動程式因本次列印文件產生的列印工作序號、列印噴墨頭之移動次數、啟動的噴墨噴孔數、使用的紙張編碼、及當時列印之總頁數。

14．如申請專利範圍第10、11、12或13項所述列印有加密資料之電子文件，前述加密資料係以一維條碼方式列印。

15．如申請專利範圍第10、11、12或13

項所述列印有加密資料之電子文件，前述加密資料係以二維條碼方式列印。

16．如申請專利範圍第10、11、12或13項所述列印有加密資料之電子文件，前述加密資料係以浮水印方式列印。

17．一種電子文件之列印加密方法，係對列印出來之電子文件賦予加密資料，並於列印之際同步傳送該加密資料予一驗證資料儲存單位儲存。

18．如申請專利範圍第17項所述電子文件之列印加密方法，該加密資料係為一文件辨識序號，由發出該電子文件之發文單位所賦予。

19．如申請專利範圍第17項所述電子文件之列印加密方法，該加密資料係為執行列印工作之印表機的序號。

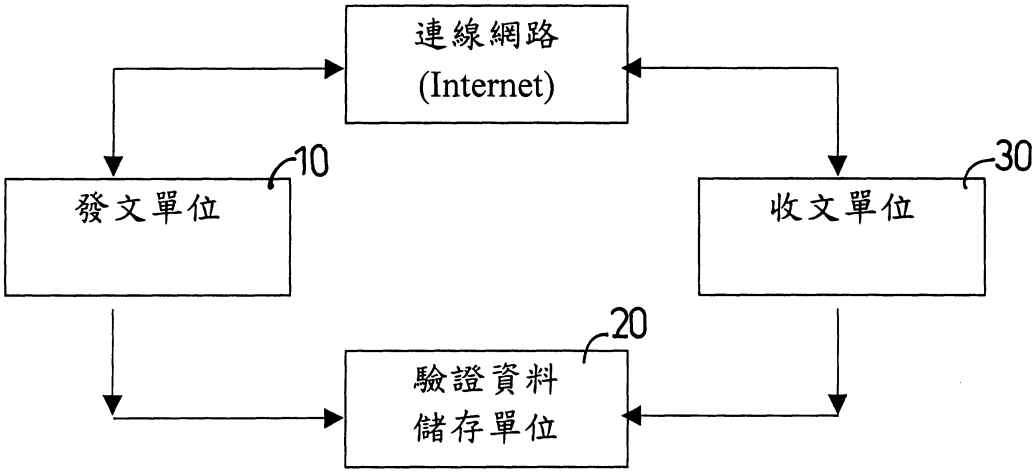
20．如申請專利範圍第17項所述列印電子文件之列印加密方法，該加密資料係為列印狀態參數。

21．如申請專利範圍第20項所述有加密資料之電子文件，前述列印狀態參數包含有列印驅動程式因本次列印文件產生的列印工作序號、列印噴墨頭之移動次數、啟動的噴墨噴孔數、使用的紙張編碼、及當時列印之總頁數。

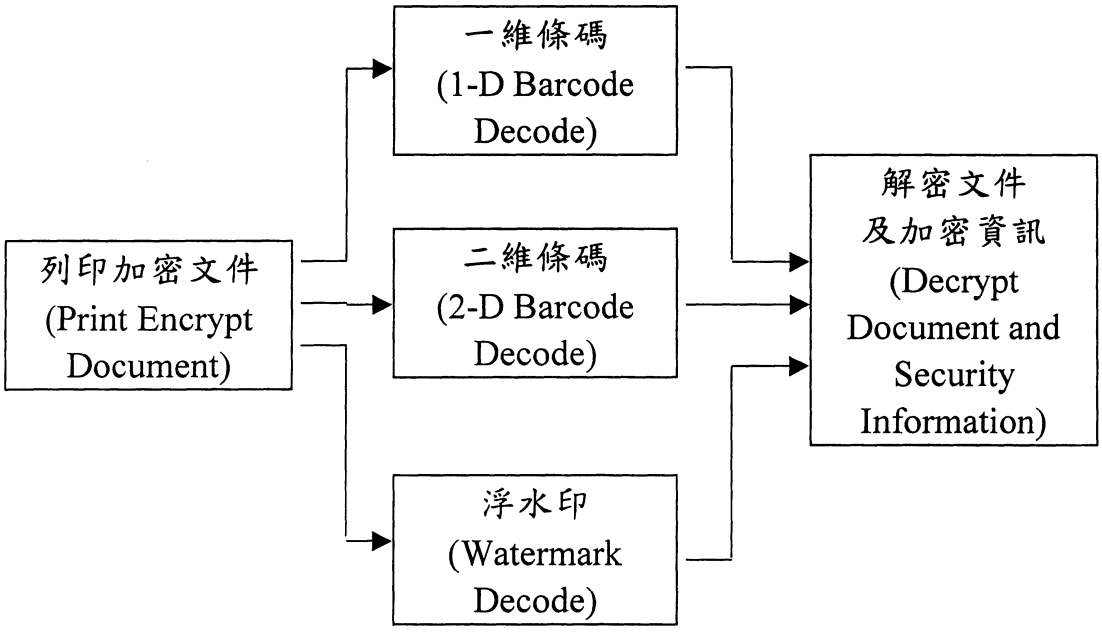
22．如申請專利範圍第18、19、20或21項所述有加密資料之電子文件，前述加密資料係以一維條碼方式列印。

２３．如申請專利範圍第１８、１９、２０或２１項所述電子文件之列印加密方法，前述加密資料係以二維條碼方式列印。

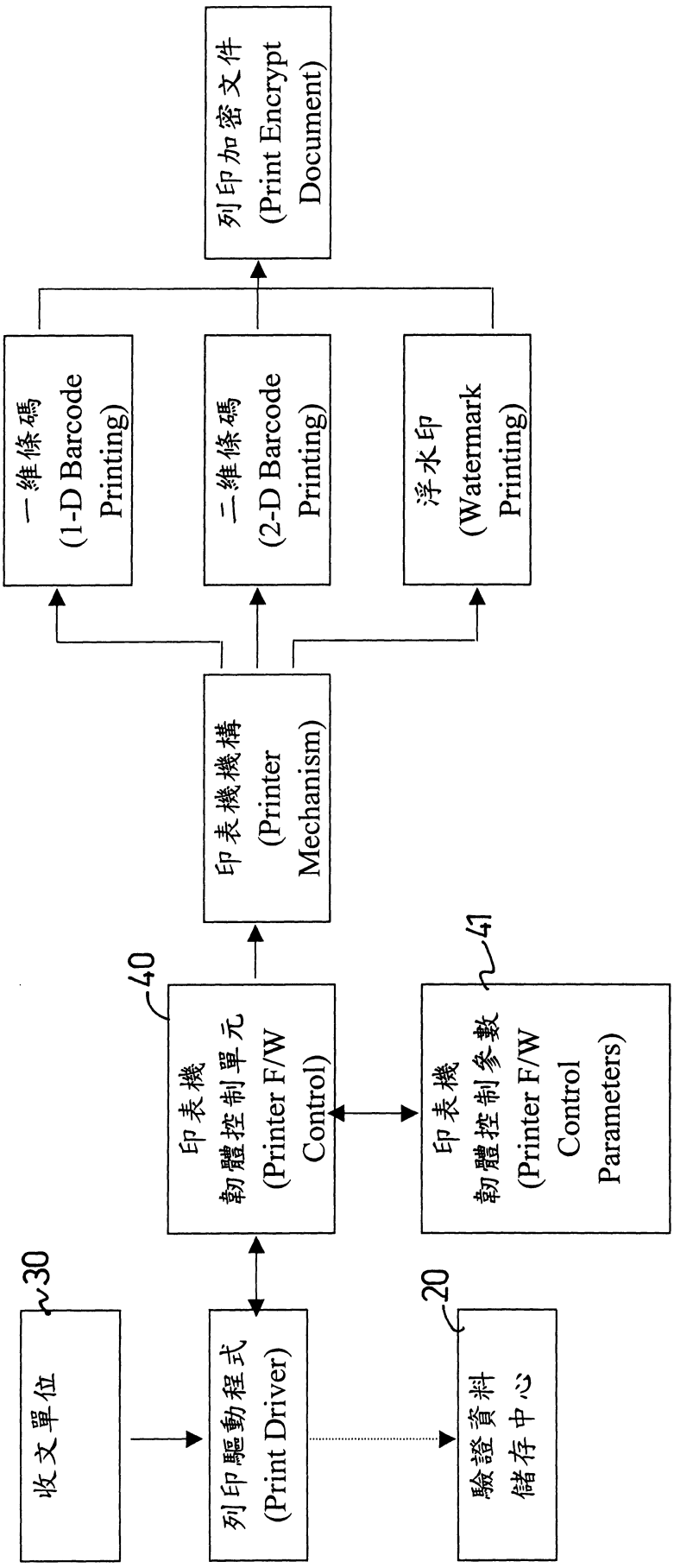
２４．如申請專利範圍第１８、１９、２０或２１項所述電子文件之列印加密方法，前述加密資料係以浮水印方式列印。


連線網路
(Internet)
10
發文單位
30
收文單位
20
驗證資料
儲存單位

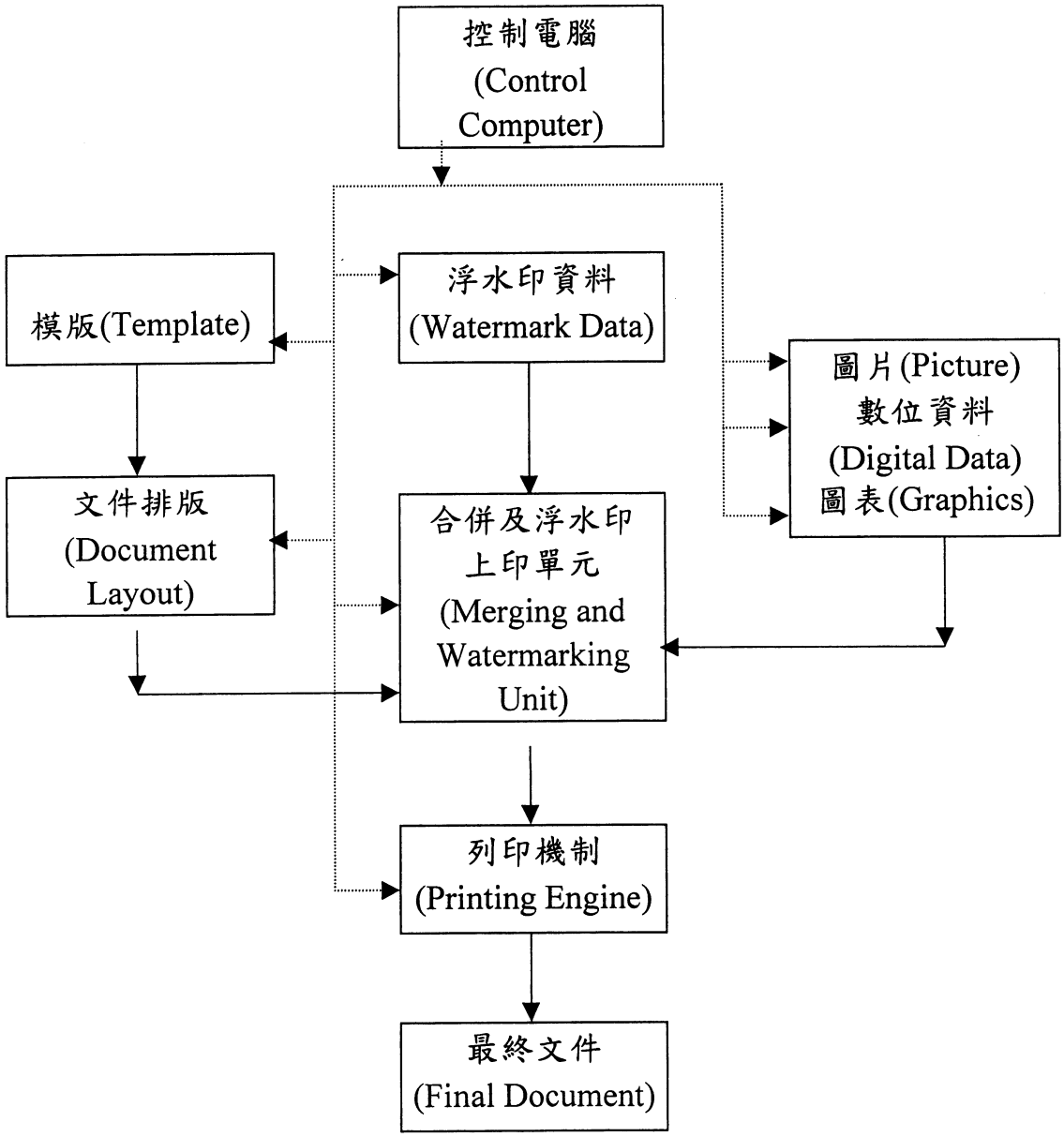
第一圖


一維條碼
(1-D Barcode
Decode)
列印加密文件
(Print Encrypt
Document)
二維條碼
(2-D Barcode
Decode)
浮水印
(Watermark
Decode)
解密文件
及加密資訊
(Decrypt
Document and
Security
Information)

第三圖


收文單位
30
列印驅動程式
(Print Driver)
20
驗證資料
儲存中心
印表機
韌體控制單元
(Printer F/W
Control)
40
印表機
韌體控制參數
(Printer F/W
Control
Parameters)
41
印表機機構
(Printer
Mechanism)
一維條碼
(1-D Barcode
Printing)
二維條碼
(2-D Barcode
Printing)
浮水印
(Watermark
Printing)
列印加密文件
(Print Encrypt
Document)

第二圖


控制電腦
(Control Computer)
模版(Template)
浮水印資料
(Watermark Data)
圖片(Picture)
數位資料
(Digital Data)
圖表(Graphics)
文件排版
(Document Layout)
合併及浮水印上印單元
(Merging and Watermarking Unit)
列印機制
(Printing Engine)
最終文件
(Final Document)

第四圖

陸、(一)、本案指定代表圖為：第 一 圖

(二)、本代表圖之元件代表符號簡單說明：

（１０）發文單位

（２０）驗證資料儲存單位

（３０）收文單位

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：