



(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 I517027 B

(45) 公告日：中華民國 105 (2016) 年 01 月 11 日

(21) 申請案號：098117989

(22) 申請日：中華民國 98 (2009) 年 06 月 01 日

(51) Int. Cl. : G06F3/12 (2006.01)

(30) 優先權：2008/05/29 世界智慧財產權組織 PCT/US08/65103

(71) 申請人：惠普研發公司 (美國) HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.

(US)

美國

(72) 發明人：雷弗史崔帕 傑考比 G REFSTRUP, JACOB GRUNDTVIG (DK)

(74) 代理人：惲軼群；陳文郎

(56) 參考文獻：

TW 532039

US 2007/0160204A1

審查人員：呂嘉雄

申請專利範圍項數：12 項 圖式數：3 共 21 頁

(54) 名稱

提供經驗證通訊內容予可更換印表機構件之技術

PROVIDING AUTHENTICATED COMMUNICATIONS TO A REPLACEABLE PRINTER
COMPONENT

(57) 摘要

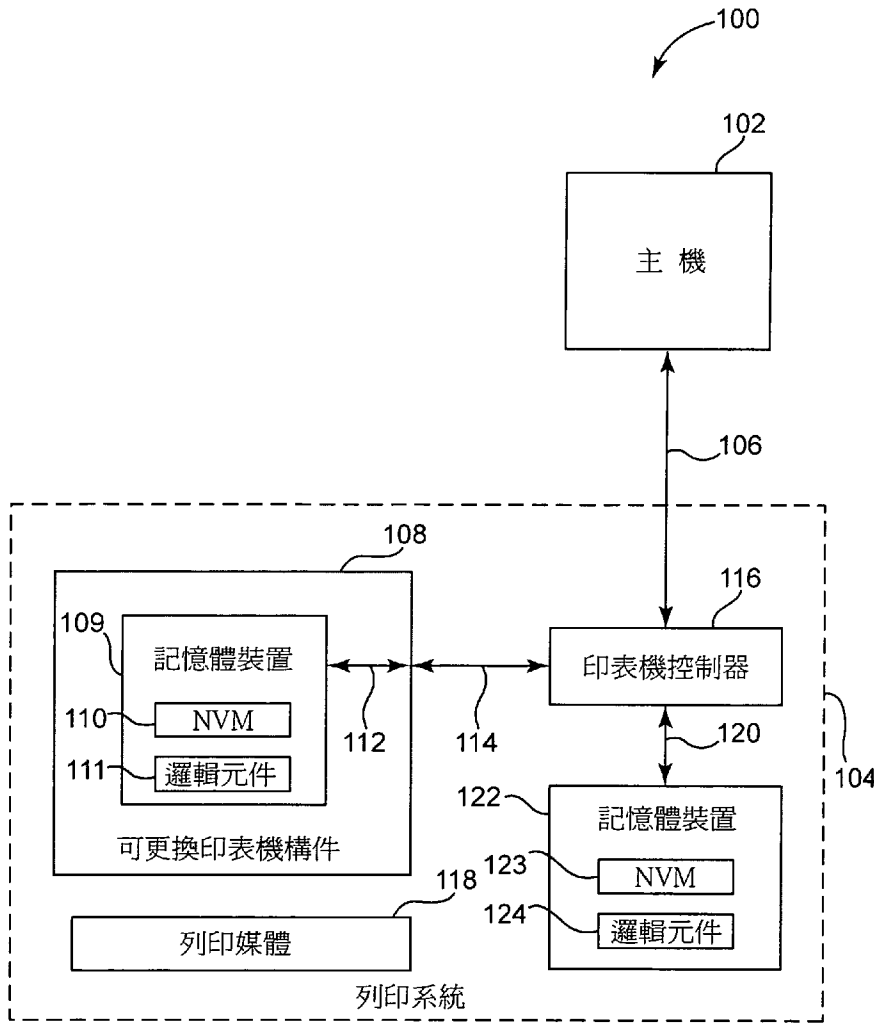
一種可更換印表機構件，其包括一第一記憶體裝置及一通訊鏈結。該第一記憶體裝置儲存一第一機密。該通訊鏈結受組配以在該可更換印表機構件安裝於一列印系統中時將該第一記憶體裝置通訊地鏈結於一印表機控制器。該列印系統包括儲存一第二機密的一第二記憶體裝置。該第二記憶體裝置通訊地鏈結於該印表機控制器。該第一記憶體裝置受組配以基於該第一機密及該第二機密驗證在該第一記憶體裝置與該印表機控制器之間的通訊內容。

A replaceable printer component includes a first memory device and a communication link. The first memory device stores a first secret. The communication link is configured to communicatively link the first memory device to a printer controller when the replaceable printer component is installed in a printing system. The printing system includes a second memory device storing a second secret. The second memory device is communicatively linked to the printer controller. The first memory device is configured to authenticate communications between the first memory device and the printer controller based on the first secret and the second secret.

指定代表圖：

符號簡單說明：

- 100 . . . 列印配置
- 102 . . . 主機
- 104 . . . 列印系統
- 106 . . . 通訊鏈結
- 108 . . . 可更換印表機構件
- 109 . . . 記憶體裝置
- 110 . . . 非揮發性記憶體/NVM
- 111 . . . 邏輯元件
- 112/114 . . . 通訊鏈結
- 116 . . . 印表機控制器
- 118 . . . 列印媒體
- 120 . . . 通訊鏈結
- 122 . . . 記憶體裝置
- 123 . . . 非揮發性記憶體/NVM
- 124 . . . 邏輯元件



第 1 圖

發明專利說明書

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：98117989

※ 申請日：98-6-1

※IPC 分類：

G06F 3/12

(2006.01)

一、發明名稱：(中文/英文)

提供經驗證通訊內容予可更換印表機構件之技術

PROVIDING AUTHENTICATED COMMUNICATIONS TO A
REPLACEABLE PRINTER COMPONENT

二、中文發明摘要：

一種可更換印表機構件，其包括一第一記憶體裝置及一通訊鏈結。該第一記憶體裝置儲存一第一機密。該通訊鏈結受組配以在該可更換印表機構件安裝於一列印系統中時將該第一記憶體裝置通訊地鏈結於一印表機控制器。該列印系統包括儲存一第二機密的一第二記憶體裝置。該第二記憶體裝置通訊地鏈結於該印表機控制器。該第一記憶體裝置受組配以基於該第一機密及該第二機密驗證在該第一記憶體裝置與該印表機控制器之間的通訊內容。

三、英文發明摘要：

A replaceable printer component includes a first memory device and a communication link. The first memory device stores a first secret. The communication link is configured to communicatively link the first memory device to a printer controller when the replaceable printer component is installed in a printing system. The printing system includes a second memory device storing a second secret. The second memory device is communicatively linked to the printer controller. The first memory device is configured to authenticate communications between the first memory device and the printer controller based on the first secret and the second secret.

四、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100...列印配置	112/114...通訊鏈結
102...主機	116...印表機控制器
104...列印系統	118...列印媒體
106...通訊鏈結	120...通訊鏈結
108...可更換印表機構件	122...記憶體裝置
109...記憶體裝置	123...非揮發性記憶體/NVM
110...非揮發性記憶體/NVM	124...邏輯元件
111...邏輯元件	

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

相互參照相關申請案

這個申請案相關於與本申請案在相同日期提出申請的 PCT 專利申請案序列號第##/###,###號案，其代理人檔案號第 200800134-1 號，其名稱為“AUTHENTICATING A REPLACEABLE PRINTER COMPONENT”，且以參照形式併入本文。

本發明係有關於提供經驗證通訊內容予可更換印表機構件之技術。

【先前技術】

發明背景

當前的列印系統典型地包括一或多個可更換印表機構件，諸系統對此等可更換印表機構件提供機載記憶體，如噴墨匣、噴墨列印頭總成、碳粉匣、墨水供應等。一些現存的以將關於該可更換構件之諸如墨水填充位準、購買資訊等資訊傳遞至一印表機。

典型地依賴儲存於一可更換印表機構件之機載記憶體中的該資料，以適當地操作及追蹤該可更換印表機構件及安裝該可更換印表機構件於其中的該列印系統。照這樣，儲存於該機載記憶體中的該資料不應遭受未經驗證使用或未經驗證修改。

對於此等及其他原因，對於本發明存在一需求。

【發明內容】

依據本發明之一實施例，係特地提出一種可更換印表機構件，其包含：一第一記憶體裝置，其儲存一第一機密；及一通訊鏈結，其受組配以在該可更換印表機構件安裝於一列印系統中時將該第一記憶體裝置通訊地鏈結於一印表機控制器，其中該列印系統包含儲存一第二機密的一第二記憶體裝置，該第二記憶體裝置通訊地鏈結於該印表機控制器，其中該第一記憶體裝置受組配以基於該第一機密及該第二機密驗證該第一記憶體裝置與該印表機控制器之間的通訊內容。

圖式簡單說明

該等附圖遭包括以提供對實施例的一進一步理解且遭合併於且構成這個說明書的一部分。該等圖式說明實施例且連同該描述一起用以解釋實施例的原理。其他實施例及許多實施例之該等所期望的優點將容易理解，當參照下面詳細的描述它們變得更容易理解時。該等圖式的元件彼此間不必按比例繪製。相同的參照數字指定相對應之相似的部分。

第1圖是說明一列印配置之一實施例的一方塊圖。

第2圖是說明用於驗證在一可更換印表機構件與一列印系統之間之通訊內容之一方法之一實施例的一流程圖。

第3圖是說明用於驗證由一列印系統發送至一可更換印表機構件之一讀取或寫入請求之一方法之一實施例的一流程圖。

【實施方式】

較佳實施例之詳細說明

在下面的詳細描述中，參照在此形成一部分的該等附圖，且本發明可實行於其中之說明特定實施例顯示於其中。在這一方面，方向術語，諸如“頂端”、“底端”、“前端”、“後端”、“前導的”、“滯後的”等參照所描述之該等圖式的方位予以使用。因為實施例的構件可定位於多個不同的方位，所以該方向術語以說明為目的予以使用且決不是限制。應理解的是可利用其他實施例且可做出結構的或邏輯的改變而不背離本發明之範圍。因此，不應該限制於下面詳細的描述，且本發明之範圍由該等附加申請專利範圍定義。

應理解的是本文所描述之該等各種示範實施例的該等特徵可相互結合，除非另外特別地說明。

第1圖是說明一列印配置100之一實施例的一方塊圖。列印配置100包括一主機102及一列印系統104。列印系統104有助於將圖形及/或文字影像列印於諸如紙、卡片、幻燈片、聚脂薄膜、布料等的一列印媒體118上。列印系統104包括例如一噴墨印表機、一雷射印表機或其他適當的印表機。主機102與列印系統104通訊且將資料及/或控制信號提供給列印系統104。主機102可以是或可包括於各種資訊源中的諸如一電腦、電器或諸如一個人數位助理(PDA)、數位照相機、行動電話等之其他適當的裝置。

在一實施例中，列印系統104包括一印表機控制器116、一記憶體裝置122及一可更換印表機構件108。可更換

印表機構件108包括一記憶體裝置109。在一實施例中，印表機控制器116基於儲存於記憶體裝置109及記憶體裝置122中的密鑰驗證在記憶體裝置109與印表機控制器116之間的通訊內容。因而，防止儲存於可更換印表機構件108之記憶體裝置109中之資料的未經授權的讀取及/或寫入。

印表機控制器116控制該列印系統104的操作且諸如接收來自主機102的資料及/或控制信號。印表機控制器116經由一通訊鏈結106與主機102通訊。通訊鏈結106包括在印表機控制器116與主機102之間的例如一電氣的、光學的、紅外線的其他適當的資訊傳送路徑。印表機控制器116經由一通訊鏈結120與記憶體裝置122通訊。通訊鏈結120包括在印表機控制器116與記憶體裝置122之間之例如一電氣的、光學的、紅外線的或其他適當的資訊傳送路徑。

記憶體裝置122包括一非揮發性記憶體(NVM)123及邏輯元件124。在一實施例中，記憶體裝置122是防竄改或抗竄改。在一實施例中，邏輯元件124是一邏輯電路或執行於一處理器上的嵌入軟體。例如，在一實施例中，記憶體裝置122包括一中央處理單元(CPU)或具有嵌入非揮發性記憶體123的系統單晶片(SoC)。在另一實施例中，記憶體裝置122包括一CPU或具有外部非揮發性記憶體123的SoC。在另一實施例中，記憶體裝置122包括具有內部或外部非揮發性記憶體123的專用邏輯元件。在另一實施例中，記憶體裝置122被嵌入具有內部或外部非揮發性記憶體123的印表機控制器116內。

在一實施例中，非揮發性記憶體123是一EEPROM、一FLASH或另外適當的記憶體。非揮發性記憶體123儲存用以驗證在印表機控制器116與可更換印表機構件108之記憶體裝置109之間之通訊內容的一或多個密鑰。印表機控制器116與記憶體裝置109之間的通訊內容藉由使用交談金鑰予以驗證。為了產生一交談金鑰，印表機控制器116將一交談金鑰識別符及對一交談金鑰的一請求傳遞至記憶體裝置122。根據該交談金鑰識別符及對一交談金鑰的該請求，邏輯電路124基於該交談金鑰識別符及儲存於非揮發性記憶體123中的一密鑰產生一交談金鑰。接著邏輯電路124將該所產生之交談金鑰提供給印表機控制器116。

可更換印表機構件108包括可插入列印系統104且從列印系統104移除之列印系統104的一構件。在一實施例中，可更換印表機構件108包括在其使用壽命的結束時棄置且更換的一消耗性構件。這樣一消耗性構件的一範例包括包含為列印系統104供應一標識材料的一墨水容器或一碳粉匣。該標識材料藉由列印系統104沈積於列印媒體118上且在該墨水容器或碳粉匣之一使用壽命期間予以耗盡。照這樣，該墨水容器或碳粉匣在其使用壽命結束時予以棄置及更換或予以再製造及再利用。

在另一實施例中，可更換印表機構件108包括在列印系統104中可輕易地更換的一列印構件。這樣一列印構件的範例包括根據來自印表機控制器116的控制信號選擇性地將墨水沈積於列印媒體118上的一列印頭或包括一列印頭及

一墨水供應的一印表機匣。因而，可更換印表機構件108可包括一墨水容器、一系列印頭或一印表機匣，如果例如列印系統104包括一噴墨印表機。此外，可更換印表機構件108可包括一碳粉匣或一顯影滾筒，如果例如列印系統104包括一雷射印表機。而且，可更換印表機構件108可包括列印系統104的一週邊裝置，諸如一乙太網路卡、一雙工器、一紙整理器(例如釘書機、打孔器等)或另外適當的裝置。

印表機控制器116與可更換印表機構件108經由一通訊鏈結114相互通訊。通訊鏈結114在可更換印表機構件108安裝於列印系統104時，有助於資訊在印表機控制器116與可更換印表機構件108之間傳送。通訊連接114包括在可更換印表機構件108與印表機控制器116之間之例如一電氣的、光學的、紅外線的或其他適當的資訊傳送路徑。

可更換印表機構件108包括儲存用於可更換印表機構件108及/或列印系統104之資訊的一記憶體裝置109。記憶體裝置109包括一非揮發性記憶體(NVM)110及邏輯元件111。在一實施例中，記憶體裝置109是防竄改或抗竄改。在一實施例中，邏輯元件111是一邏輯電路或執行於一處理器上的嵌入軟體。例如，在一實施例中，記憶體裝置109包括一CPU或具有嵌入非揮發性記憶體110的SoC。在另一實施例中，記憶體裝置109包括一CPU或具有外部非揮發性記憶體110的SoC。在另一實施例中，記憶體裝置109包括具有內部或外部非揮發性記憶體110的專用邏輯元件。

在一實施例中，非揮發性記憶體110是一個256位元組

或另外適當大小的非揮發性記憶體，諸如一EEPROM、一FLASH或另外適當的記憶體。在一實施例中，記憶體裝置109之非揮發性記憶體110儲存例如對可更換印表機構件108特定的資訊及/或適用於列印系統104的資訊。此外，非揮發性記憶體110中可儲存有由列印系統104所使用之資訊或可記錄用於列印系統104之資訊。在一實施例中，可儲存於非揮發性記憶體110中的資訊包括可更換印表機構件108及/或列印系統104之操作的及/或非操作的參數。

非揮發性記憶體110還可儲存用以驗證記憶體裝置109與印表機控制器116之間之通訊內容的一或多個密鑰。在一實施例中，儲存於記憶體裝置109之非揮發性記憶體110中的該等一或多個密鑰源於儲存於記憶體裝置122之非揮發性記憶體123中的該等一或多個密鑰。在其他實施例中，儲存於記憶體裝置109之非揮發性記憶體110中的該等一或多個密鑰與儲存於記憶體裝置122之非揮發性記憶體123中的該等一或多個密鑰源於一或多個共用的密鑰。照這樣，儲存於非揮發性記憶體110中的該等一或多個密鑰相關於儲存於非揮發性記憶體123中的該等一或多個密鑰。

在一實施例中，可更換印表機構件108包括在可更換印表機構件108安裝於列印系統104中時，使記憶體裝置109與通訊鏈結114且從而與印表機控制器116電氣耦接或通訊地耦接的一通訊鏈結112。照這樣，當可更換印表機構件108安裝於列印系統104中時，記憶體裝置109經由通訊鏈結112及114與印表機控制器116通訊。因而，通訊鏈結112及114

包括例如電氣耦接或連接體，諸如分別與相對應之電氣節點或插座相接合之電氣接頭或接腳。

記憶體裝置109與印表機控制器116之間的通訊內容藉由使用交談金鑰予以驗證。為了產生一交談金鑰，印表機控制器116將對一交談金鑰識別符的一請求傳遞至記憶體裝置109。根據對一交談金鑰識別符的該請求，記憶體裝置109的邏輯電路111基於儲存於非揮發性記憶體110中的一密鑰產生一交談金鑰識別符及一相關聯之交談金鑰。在一實施例中，記憶體裝置109的邏輯電路111根據一交談金鑰識別符之各請求產生一不同的交談金鑰識別符及一相關聯之交談金鑰。因此，各交談金鑰識別符及各相關聯之交談金鑰僅能使用一次。邏輯電路111將該所產生之交談金鑰識別符提供至印表機控制器116，其如以上之先前描述將該交談金鑰識別符依次傳遞至記憶體裝置122。

第2圖是說明用於驗證在一可更換印表機構件108與一系列印系統104之間之通訊內容之一方法150之一實施例的一流程圖。在152處，一可更換印表機構件108安裝於包括一印表機控制器116的一系列印系統104中。該可更換印表機構件108包括已組配有用於驗證與列印系統104之通訊內容的一或多個密鑰的一記憶體裝置109。該列印系統104還包括已組配有用於驗證與可更換印表機構件108之通訊內容的一或多個密鑰的一記憶體裝置122。

在154處，印表機控制器116經由通訊鏈結114及112向可更換印表機構件108之記憶體裝置109請求一交談金鑰識

別符。在156處，根據接收對一交談金鑰識別符的該請求，記憶體裝置109之邏輯電路111基於儲存於非揮發性記憶體110內的一第一密鑰產生該所請求之交談金鑰識別符及其相關聯之交談金鑰。在158處，記憶體裝置109之邏輯電路111將該所請求之交談金鑰識別符提供給印表機控制器116。

在160處，印表機控制器116將從記憶體裝置109所接收的該交談金鑰識別符透過通訊鏈結120提供給記憶體裝置122且請求一交談金鑰。在162處，根據接收該交談金鑰識別符及對一交談金鑰的該請求，記憶體裝置122之邏輯電路124基於該所接收之交談金鑰識別符及儲存於非揮發性記憶體123中的一第二密鑰產生該所請求的交談金鑰。如果儲存於記憶體裝置109之非揮發性記憶體110中的該第一密鑰相關於儲存於記憶體裝置122之非揮發性記憶體123中的該第二密鑰，那麼由邏輯電路111所產生之該交談金鑰與由邏輯電路124所產生之該交談金鑰相匹配。在164處，記憶體裝置122之邏輯電路124將該所請求之交談金鑰提供給印表機控制器116。在166處，印表機控制器116使用該所接收之交談金鑰以驗證在印表機控制器116與可更換印表機構件108的記憶體裝置109之間的通訊內容。

第3圖是說明用於驗證由一列印系統104發送至一可更換印表機構件108之一讀取或寫入請求之一方法166的一實施例的一流程圖。在170處，利用在可更換印表機構件108之記憶體裝置109中所建立的一交談金鑰及在列印系統104

中所建立的一交談金鑰，印表機控制器116使用其交談金鑰及一適當的密碼演算法為一讀取或寫入請求計算一第一訊息驗證碼(MAC)。該第一MAC對該讀取或寫入請求的該命令及命令參數予以計算。在一實施例中，一MAC分集器用於該第一MAC的該計算中以防止重播攻擊記憶體裝置109。

在一實施例中，該第一MAC基於具有諸如安全雜湊演算法1(SHA-1)、SHA-2或其他適當之安全雜湊演算法之一安全雜湊的一雜湊訊息驗證碼(HMAC)予以計算。在另一實施例中，該第一MAC基於具有諸如資料加密標準(DES)、3DES、先進加密標準(AES)、Rivest密碼法2(RC2)之一密碼區塊演算法或其他適當的密碼區塊演算法的一基於密碼的MAC(CMAC)予以計算。在其他實施例中，該第一MAC使用另外適當的技術予以計算。

在172處，印表機控制器116將包括該第一MAC的讀取或寫入請求發送至可更換印表機構件108之記憶體裝置109。在174處，根據該讀取或寫入請求，記憶體裝置109之邏輯電路111使用其交談金鑰及該加密演算法對於該所接收之讀取或寫入請求計算一第二MAC。在176處，記憶體裝置109之邏輯電路111將該所接收之第一MAC與該所計算之第二MAC進行比較。

在178處，如果該第一MAC與該第二MAC相匹配，那麼記憶體裝置109的該交談金鑰與列印系統104的該交談金鑰相匹配。因此，記憶體裝置109與印表機控制器116之間的該通訊內容獲驗證。在180處，記憶體裝置109之邏輯電

路111執行該所請求之讀取或寫入操作。使用該等所建立之交談金鑰，對於各附加的讀取或寫入請求，重複方法170直至該通訊內容交談結束。該通訊內容交談可藉由印表機控制器116或藉由列印系統104及/或可更換印表機構件108的一電力損耗而結束。

在178處，如果該第一MAC與該第二MAC不相匹配，那麼記憶體裝置109的該交談金鑰與列印系統104的該交談金鑰不相匹配。因此，記憶體裝置109與印表機控制器116之間的該通訊內容未獲驗證。在182處，記憶體裝置109之邏輯電路111中斷或拒絕該所請求之讀取或寫入操作。在184處，記憶體裝置109之邏輯電路111將其交談金鑰標記為無效使得它不能再一次予以使用。

實施例提供了一可更換印表機構件可安裝於其中的一列印系統。列印系統實施例包括儲存一或多個密鑰的一記憶體裝置。可更換印表機構件實施例包括儲存與儲存於該等列印系統實施例之該記憶體裝置中之該等一或多個密鑰相關之一或多個密鑰的一記憶體裝置。儲存於該等列印系統實施例及該等可更換印表機構件實施例中的該等一或多個密鑰用以驗證在該等列印系統實施例與該等可更換印表機構件實施例之間的通訊內容。

雖然特定的實施例已經被說明並被描述於此，但是在該技藝中具有通常知識者將理解的是，各種供選擇的及/或等效的實施可代替所顯示之該等特定的實施例且予以描述而不背離本發明之範圍。此申請案企圖涵蓋在此所討論之

該等特定實施例的任何的改作或變化。因此，其企圖在於此發明僅受其該等申請專利範圍及該等等效物限制。

【圖式簡單說明】

第1圖是說明一系列印配置之一實施例的一方塊圖。

第2圖是說明用於驗證在一可更換印表機構件與一系列印系統之間之通訊內容之一方法之一實施例的一流程圖。

第3圖是說明用於驗證由一系列印系統發送至一可更換印表機構件之一讀取或寫入請求之一方法之一實施例的一流程圖。

【主要元件符號說明】

100...列印配置	118...列印媒體
102...主機	120...通訊鏈結
104...列印系統	122...記憶體裝置
106...通訊鏈結	123...非揮發性記憶體/NVM
108...可更換印表機構件	124...邏輯元件
109...記憶體裝置	150...方法
110...非揮發性記憶體/NVM	152~166...步驟
111...邏輯元件	166...方法
112/114...通訊鏈結	170~184...步驟
116...印表機控制器	

七、申請專利範圍：

1. 一種可更換印表機構件，包含：

一第一記憶體裝置，其儲存一第一機密；及

一通訊鏈結，其組配來在該可更換印表機構件安裝於一列印系統中時，將該第一記憶體裝置通訊地鏈結於一印表機控制器，

其中該第一記憶體裝置係組配來：

基於該第一機密產生一交談金鑰識別符及一第一交談金鑰，並且響應於一請求而提供該交談金鑰識別符至該印表機控制器；

接收來自該印表機控制器的一讀或寫的請求，該讀或寫的請求係包括一第一訊息驗證碼，該第一訊息驗證碼係使用基於該交談金鑰識別符及一第二機密的一第二交談金鑰所計算出；及

基於來自該印表機控制器的該讀或寫的請求以及該第一交談金鑰，計算一第二訊息驗證碼，並響應於該第二訊息驗證碼與該第一訊息驗證碼相符合，執行該讀或寫的請求。

2. 如申請專利範圍第1項所述之可更換印表機構件，其中該第一機密係源於該第二機密。

3. 如申請專利範圍第1項所述之可更換印表機構件，其中該第一記憶體裝置為防竄改的記憶體裝置。

4. 如申請專利範圍第1項所述之可更換印表機構件，進一步包含一噴墨匣、一噴墨列印頭總成、一碳粉匣及一墨水

供應源其中之一者。

5. 如申請專利範圍第1項所述之可更換印表機構件，進一步包含該列印系統的一周邊裝置。
6. 一種列印系統，包括：
 - 5 如申請專利範圍第1項所述之可更換印表機構件，該印表機控制器，及一第二記憶體裝置，儲存該第二機密，該第二記憶體裝置通訊地鏈結至該印表機控制器，並組配來基於該交談金鑰識別符及該第二機密產生第二交談金鑰。
 - 10 7. 如申請專利範圍第6項所述之列印系統，其中該第一記憶體裝置係組配來接收來自該印表機控制器的讀或寫請求，該讀或寫請求包括使用該第二交談金鑰計算出的一第一訊息驗證碼，且其中，該第一記憶體裝置係組配來基於該讀或寫請求以及該第一交談金鑰而計算第二訊息驗證碼，並且響應於該第二訊息驗證碼與該第一訊息驗證碼相符合，而執行該讀或寫的請求。
 - 15 8. 如申請專利範圍第7項所述之列印系統，其中該第一記憶體裝置係組配來響應於該第二訊息驗證碼與該第一訊息驗證碼不相符合，拒絕該讀或寫請求並且標記該第一交談金鑰為無效。
 - 20 9. 如申請專利範圍第6項所述之列印系統，其中該第一記憶體裝置係組配來響應於每一個請求，產生一不同的交談金鑰識別符與交談金鑰。

10. 一種用於在可更換印表機構件與列印系統間驗證通訊的方法，包含：

可更換印表機構件儲存一第一密鑰；

使該可更換印表機構件安裝於列印系統中，該列印系統儲存一第二密鑰；

請求來自該可更換印表機構件之一交談金鑰識別符；

響應於該請求，在該可更換印表機構件中基於該第一密鑰產生該交談金鑰識別符及一第一交談金鑰；

在該列印系統中，基於該交談金鑰識別符及該第二密鑰，產生一第二交談金鑰；

在該列印系統中，為針對該可更換印表機構件的讀或寫請求，使用該第二交談金鑰計算一第一訊息驗證碼；

對該可更換印表機構件發出包括該第一訊息驗證碼的讀或寫請求；

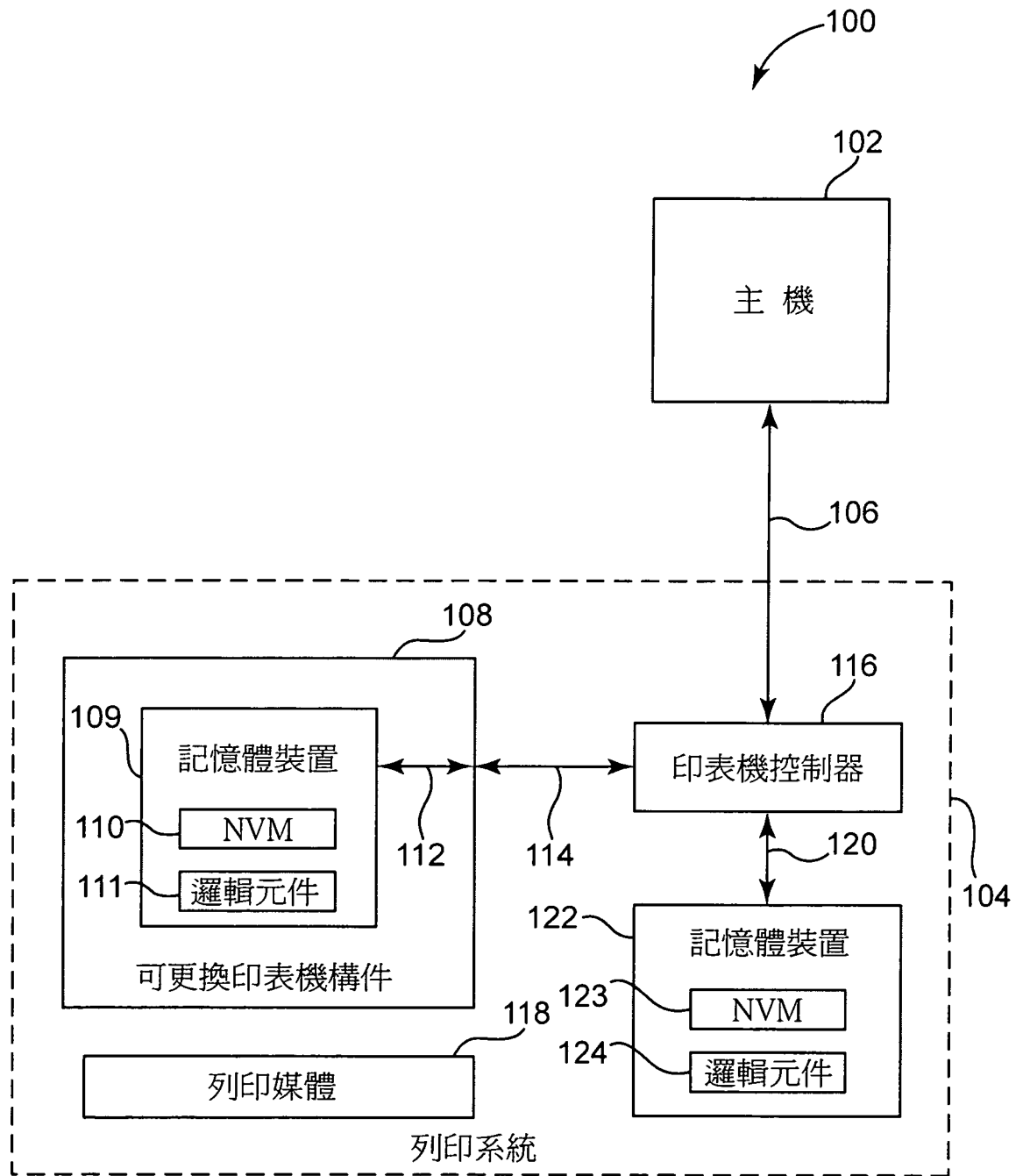
在該可更換印表機構件中，使用該第一交談金鑰計算用於該讀或寫請求的一第二訊息驗證碼；及

響應於該第二訊息驗證碼與該第一訊息驗證碼相符合，執行該讀或寫的請求。

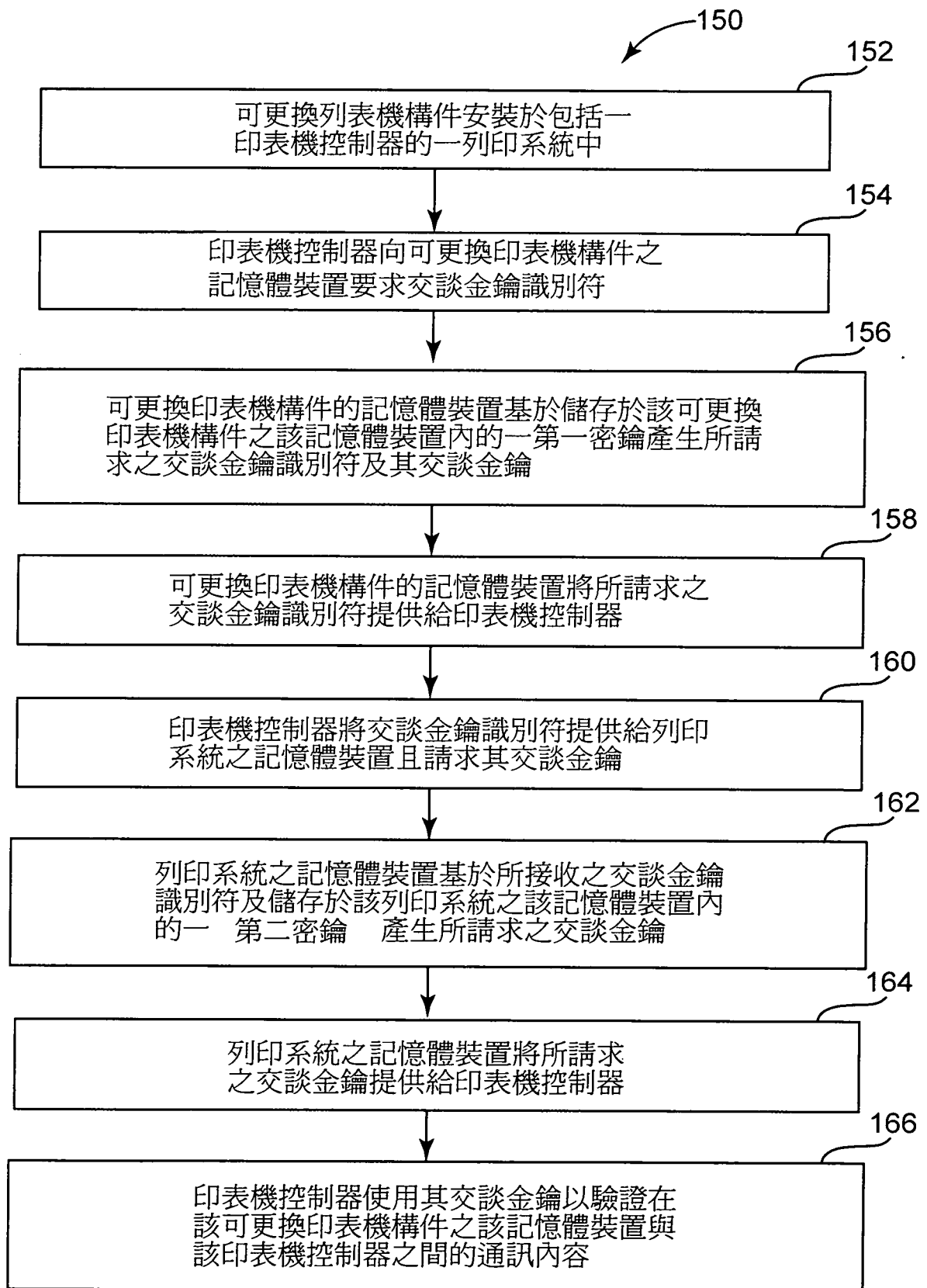
11. 如申請專利範圍第10項所述之方法，其中該第一密鑰係源於該第二密鑰。

12. 如申請專利範圍第10項所述之方法，還包含：響應於該第二訊息驗證碼與該第一訊息驗證碼不相符合，拒絕該

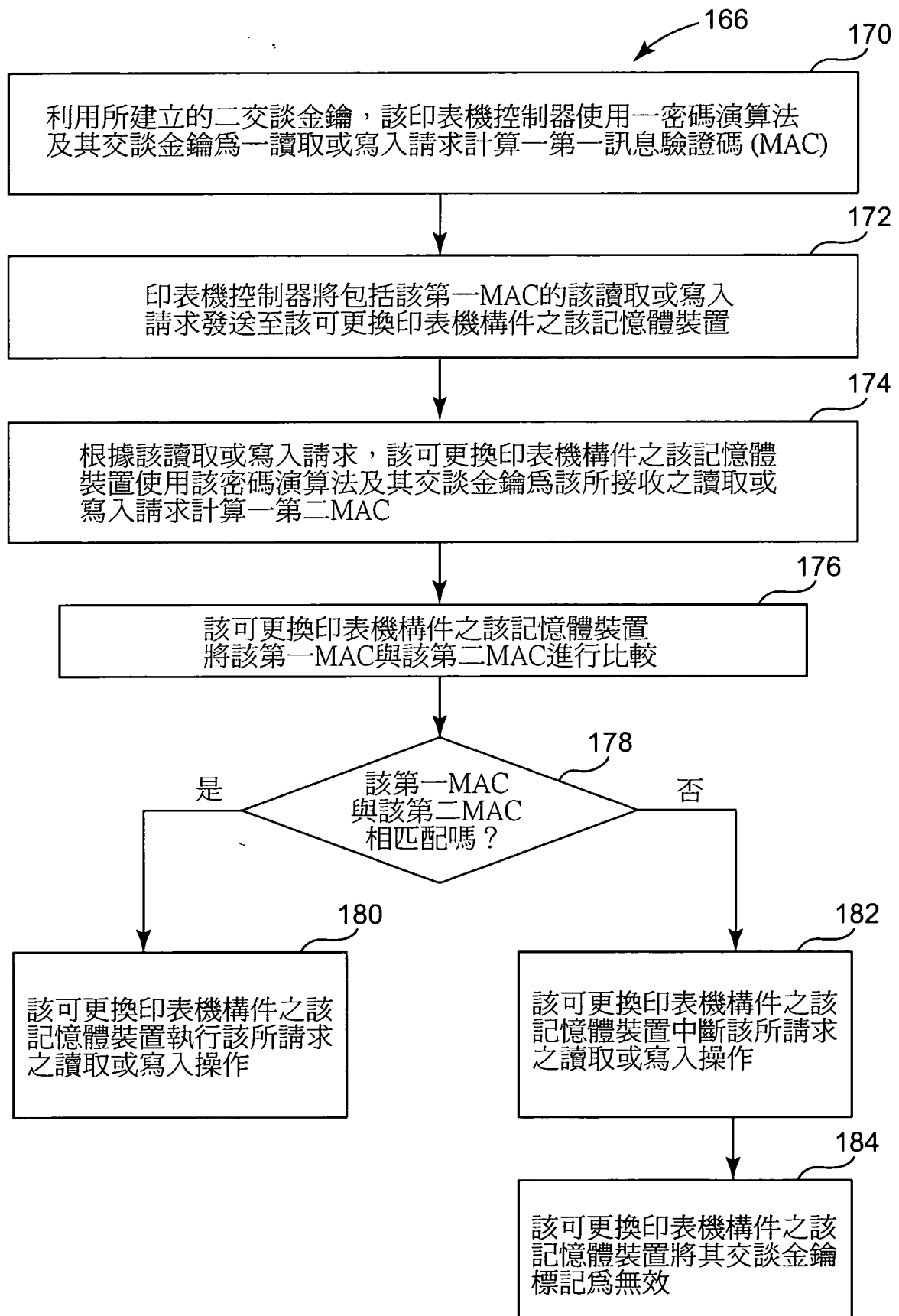
讀或寫請求並且標記該第一交談金鑰為無效。



第 1 圖



第 2 圖



第 3 圖