I438698

（此處由本局於收文時黏貼條碼）

公告本

764192

發明專利說明書

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：95147699

※申請日期：95年12月19日　　※IPC分類：G06K19/10 (2006.01)

一、發明名稱：

(中) 可判別真僞之卡片

(英)

二、申請人：(共 1 人)

1.姓　名：（中）國際先端技術總合研究所股份有限公司
（英）INTERNATIONAL FRONTIER TECHNOLOGY LABORATORY, INC.
代表人：（中）1.小松信明
（英）1.KOMATSU, NOBUAKI
地　址：（中）日本國東京都千代田區永田町二丁目一〇番二號　秀和永田町ＴＢＲ大樓
（英）ShuwaNagatacho TBR Bldg., 10-2, Nagata-cho, 2-chome, Chiyoda-ku, Tokyo 100-0014 Japan
國籍：（中英）日本　　JAPAN

三、發明人：(共 2 人)

1.姓　名：（中）小松信明
（英）KOMATSU, NOBUAKI
國　籍：（中）日本
（英）JAPAN

2.姓　名：（中）南條真一郎
（英）NANJO, SHIN-ICHIRO
國　籍：（中）日本
（英）JAPAN

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利□主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.日本　　；2005/12/19；2005-365416 ☑有主張優先權
2.日本　　；2006/07/24；2006-200823 ☑有主張優先權

3.日本 ；2006/10/23 ；2006-287714 ☑有主張優先權

五、中文發明摘要

發明之名稱：可判別真偽之卡片

[課題]防止偽造卡片之使用。

[解決手段]將記載有無法複製或是難以複製之資訊的真偽認證晶片安裝於卡片，並在對卡片處理之裝置內附加卡片真偽認證處理裝置。於卡片內安裝真偽證明晶片，其係記載有將被記載於真偽認證晶片中之資訊作數位化後的資料加密化後之加密化資料，並經由真偽證明晶片來確認真偽認證晶片的正當性。在開始密碼的輸入等之具體操作之前，判定卡片之真偽，並將偽造卡片排除。

六、英文發明摘要

發明之名稱：

七、指定代表圖

（一）、本案指定代表圖為:第（ 22 ）圖

（二）、本代表圖之元件代表符號簡單說明：無

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(1)

九、發明說明

【發明所屬之技術領域】

本申請案之發明，係爲有關於例如卡片、紙幣、證券類等之易於僞造，而成爲有必要作真僞認證的對象物之構造，以及用以判別此對象物之真僞的方法者。

【先前技術】

在被稱爲卡片社會的現代，係有多種之卡片流通，而像是銀行之金融卡、信用卡公司之信用卡等有關於持有者之財產的卡片；身爲有價證券之預付卡；以及駕駛執照、健保卡、護照等之相關於身份之證明的卡片係被使用。

大多數有關於財產之卡片以及身爲有價證券之卡片，係在被設置於表面又或是背面之磁性條內寫入有必要之資訊，並使用 ATM（Automatic Teller's Machine）等之自動機械或是手動之讀取裝置，而從磁性條讀取磁性資訊，並實行各種之處理。

於圖 1 所示，係爲現在之金融卡處理流程的例子。

（1）若是卡片之持有者將金融卡插入 ATM 等之終端裝置的卡片插入口內，則卡片插入口之感測器係感測有此，而將卡片取入至裝置內。

（2）當取入卡片時，終端裝置係從卡片之磁性記錄部而讀取卡片資訊。在金融卡之情況，係讀取銀行代碼、分店代碼、帳戶種類、帳戶號碼等的卡片資訊。另外，在信用卡的情況，係將卡片識別號碼、有效期限、帳戶種類

(2)

、帳戶號碼等作爲卡片資訊，而記錄於磁性記錄部。又，亦有在金融卡或是信用卡中記錄有密碼的情況，此時係亦對密碼作讀取。

（3）終端裝置，係判斷被插入之卡片是否爲此終端裝置所能處理的卡片。

（4）當從所讀取之卡片資訊中，無法確認有顯示此卡片係爲可處理的資訊的情況，又或是雖然係爲正當之卡片，卻因爲破損又或是污損等而造成無法讀取出卡片之資訊時，則終端裝置係將此卡片作爲無法處理之不適當卡片而排出之。

（5）當卡片係爲正當者，且磁性記錄部之資訊亦被正常地讀取出時，則開始與主電腦之通訊。

（6）從主電腦而被要求作密碼之輸入。

（7）使用者對應於主電腦之要求而將密碼輸入。

（8）若是卡片使用者對應於由主電腦而來之要求而輸入密碼，則主電腦係將所輸入之密碼，與被儲存於主電腦內之對應於所讀取之卡片資訊的密碼作比較。，

（9）當兩者不一致時，將此事記錄於卡片之磁性記錄部內，並再度要求密碼之輸入，若是再度輸入之密碼係爲正當者，則進行其後之手續，而若是仍爲不一致，則再度要求密碼之輸入，當密碼之錯誤輸入次數累積至 3 次時，則使卡片成爲無效並進行將其收入終端裝置等之無效處分。

（10）當兩者一致時，主電腦係判斷卡片使用者爲正

(3)

確之卡片擁有者，並要求對提款金額之輸入。

（11）使用者輸入提款之要求金額。

（12）若是提款要求金額係爲合適，則送出此金額之現金，並將金融卡從終端裝置排出，進行對存摺之記帳或是處理明細表之發行，而結束交易。

另外，當密碼被記錄於金融卡時，係將其密碼作爲正確者並進行交易，但是其後係從磁性記錄部將其密碼消除。

於圖 2（a）所示，係爲在圖 1 所示之現在之金融卡處理流程中被使用的金融卡之例子。於此圖中，1 係爲由塑膠等所成之金融卡本體，而於其表面側係被形成有：被記錄有資訊之磁性條 2，以及標示金融卡之插入方向的箭頭 3。另外，於圖示雖係省略，但是必要事項係以壓花（emboss）文字而被揭載。

被寫入於磁性條之資訊，由於係藉由被稱爲刷讀器（skimmer）之裝置而可容易地讀取，因此僞造卡片係被作成，且不時有僞造卡片被使用而產生被害。

而作爲其對策，內藏有半導體記憶體之 IC 卡片，係成爲代替磁性卡片者而開始被使用，且銀行等機構亦計畫將其普及化。

但是，就算是此種 IC 卡，將被保存於記憶體之資訊作讀取一事係亦爲可能，在僞造係花費時間及苦心而進行的情況下，並不能說是絕對的安全。再加上，相較於磁性卡片，IC 卡片係極爲高價，因此並不能期待其能迅速地普

及。

在銀行之金融卡的情況，雖係只需要可以在 1 個國家中使用即爲足夠，但是在信用卡的情況，係有必要成爲在外國亦能使用，因此，將在世界中所被使用之所有身爲磁性卡片之信用卡，全部替換爲規格統一之 IC 卡片一事，事實上係爲不可能。

進而，在金融卡以及信用卡中，係被作壓花加工而記錄並設置有持有者名字等的資訊，由於此些之資訊亦被使用於磁性資訊，因此壓花資訊係成爲僞造卡片作成時之線索及依據。

當此些之磁性卡片或是 IC 卡片被遺失又或是遭到盜取的情況，持有者雖易於察覺此事實，但是當被盜取後又回到持有者手中之情況，特別是不使其察覺到有被竊取過的事實而返回手中的情況時，係容易產生因僞造卡片之使用所致的被害。，

不由防止卡片之僞造來對不正當之使用作防止，而作爲用以判定卡片使用者之合適與否之手段，到目前爲止係使用有以 4 位數字所構成之密碼。但是於此些密碼中，係時常被使用有容易推測之號碼，而到目前爲止，係產生了相當多的被害。而最近，不只是採用推測手段，而更進行有藉由盜拍等之手段來對密碼作偷看，因此藉由密碼來對不正當使用作防止一事係變得極爲困難。

爲了防止僞造卡片所造成的被害，在一部份之卡片中，係採用有利用圖案認識技術之生物辨識（bio merics）

的技術。作爲生物辨識技術中之代表者，係有虹彩判別、指紋判別、掌紋判別、指靜脈判別、手掌靜脈判別、指甲靜脈判別等，在這些之中，除了虹彩判別之外的判別，係分有接觸型和非接觸型，但是不論是何者，均有必要事先將圖案作登錄，而圖案之登錄係耗費時間與勞力，並在作判別時亦爲費時，因此其運用成本變大。

在接觸型的情況時，由於有必要直接碰觸檢測裝置，因此係有在衛生上以及生理上之不快感的問題。又，當判別部分係負傷時，或是在最糟糕的情況下之失去了判別部分時，生物辨識係成爲不可能。又，在判別過程中，由於係僅作了部分之判別，因此並不能說是萬無一失者。

又，在僅有卡片持有者本人才能使用的生物辨識系統中，若是使用者並沒有使用卡片的時間，或是在身邊沒有卡片處理裝置，而希望由代理人來進行卡片之處理時，則係成爲不可能，關於此點，對使用者而言係爲不便。

作爲僞造防止的其中一個手段，係爲在信用卡、紙幣、證券類等上，附加有形成凹凸之壓花全像圖。由於複製此壓花全像圖一事係極爲困難，因此僞造附加有壓花全像圖之卡片一事事實上係爲不可能，但是在現在的使用形態中，由於係僅爲由人來對其一眼掃過而進行讀取，因此若是僞造使用有與其類似之壓花全向圖的卡片，則係爲可能。

於圖 2（b）中所示，係爲藉由感官來進行卡片之真僞認證的附加有全像圖之信用卡的例子。於此圖中，1 係爲

由塑膠等所成之信用卡本體，而於其表面側係被形成有：被記錄有資訊之磁性條 2，以及標示信用卡之插入方向的箭頭 3。另外，於圖示雖係省略，但是必要事項係以壓花（emboss）文字而被揭載。

此信用卡 1 係將被記載有箭頭 3 之部分作爲前端而被插入終端裝置，但在其前端部分附近，係被安裝有例如以壓花全像圖所構成之真僞認證晶片 4。

而在信用卡之情況，雖和金融卡不同，而係在卡片之背面設置有磁性條，但是由於對卡片之終端裝置的插入方向係爲相同，因此其結果，信用卡之磁性資訊的讀取方向，係成爲和金融卡相反。

真僞認證晶片 4，係經由將卡片插入終端裝置之操作者，而將所例示之圖案「A」，以目視，亦即是以感官而作確認，而並不會以卡片終端裝置來作讀取。

藉由感官所作的真僞認證，由於在作判別者之個人能力上係有差異，以及就算是同一人，亦會因爲判別環境以及心理狀態、生理狀況等而產生偏差等的原因，故而在作爲第 1 線的監視上雖係可發揮很大的效果，但是其信賴性係爲低。

而藉由補助器具所進行之真僞認證，則是將使用細微畫線、特殊畫線、微型文字、特殊形狀網版（screen）等，藉由使用放大鏡等之擴大器具，又或是藉由使用產生光學之干涉的特殊濾鏡，而進行真僞認證。

具體而言，係將發光基材、發光層壓薄膜、發光墨水

、熱致變色墨水、光致變色墨水等之顯示有特殊之光學特性的材料，混入基材、層壓薄膜、墨水等之中，而使用有特殊濾鏡、紫外線燈管等之補助器具者，但是此些之最終的判別，亦係依賴人類的感官，因此信賴性低。

在機械處理所致之真僞認證中，係爲將材料所持有之特性作機械性之檢測而進行真僞認證者，作爲檢測對象，係有磁性、光學特性等之檢測。

具體而言，係將發光材料、磁性材料混入基材、層壓薄膜、墨水等，而使用檢測機器者，或是將加密化後之特定的資訊，藉由 OCR 文字、磁性條碼等而作磁性的或是光學的附加，並使用磁性、光學檢測機器者。

作爲機械處理所致之真僞認證技術，在「金融業務與人工物特徵辨識」（日本銀行金融研究所）（http://www.imes.boj.or.jp/japanese/jdps/2004/04-J-12.pdf）以及「第 6 次資訊安全研討會「金融領域中之人工物特徵辨識」之情況」（http:// www.imes.boj.or.jp/japanese/kinyu/2004/kk23-2-6.pdf）中，係展示有代替生體固有的資訊，而利用被隨機配置於媒體中且不具有再現性之人工物的人工物特徵辨識系統（artifact-metric system）。

人工物特徵辨識，係利用粒狀物之光反射圖案、光纖之光透過圖案、聚合體纖維之視差畫像圖案、纖維之畫像圖案、磁性纖維之磁性圖案、隨機記錄之磁性圖案、磁性條之隨機磁性圖案、記憶胞之隨機電荷量圖案、導電性纖維之共振圖案、振動薄片之共鳴圖案等偶然所形成之圖案

。

成爲卡片之不正當使用或僞造對象的事項中，係有在將卡片發給利用者時所附加之「卡片記載資訊」、以及在卡片之製造工程中所附加之「卡片本體資訊」。（「聯合IC卡片卷面之僞造防止技術手冊」，財務省印刷局，參考（http://www.npb.go.jp/ja/info/ichb.pdf））。

卡片記載資訊，係爲對於卡片本體之在發給卡片時所印刷、附加的資訊，相當於持有人資訊、有效期限等的有關於發給的資訊。作爲不正當使用之代表的改竄，係爲將卡片記載資訊之全部、又或是一部份的記載資訊作改寫的行爲，藉由消去正規的資訊，而加寫入不正當的資訊而進行之。

卡片本體資訊，係指從所發給之卡片中去除卡片記載資訊之後的卡片本身所具備之資訊，而係指卡片的物理形狀、主要是在前印刷工程中所附加之背景花樣、基底之印刷層以及保護層壓層等，附隨於卡片本體的資訊。

僞造，係爲針對卡片本體所進行之不正當行爲，藉由對身爲附隨於卡片本體之資訊的圖案或是花樣等作複印又或是模仿，以製作外觀上近似之卡片而進行，具體而言，係將被附加於真正之卡片上的圖案或是花樣，藉由掃描器等來讀取，並添加加工修正等，而使用印表機等來進行。

對於卡片本體之僞造對策技術，就算是限定在印刷技術，亦依印刷方式、墨水、印刷花樣之組合，而存在有多數，於現今並不存在有決定性的技術。

用以判別僞造之真僞認證方法，大致可分爲：藉由感官所進行者、藉由補助器具所進行者、以及藉由機械處理所進行者。

藉由感官所進行之真僞認證，係爲以視覺、觸覺等之人類的感官來判別真僞者，藉由視覺所判別者，係有本體之色彩、浮水印、經由改變注視之角度而使所附加之花樣或色彩等產生變化的全像圖等，藉由觸覺所判別者，係有對所附加之凹凸形狀的檢測，以及對卡片本體之質感的檢測等。

具體而言，係爲如標誌（logomark）、特殊字形、防複印畫線、特色墨水、全像圖、光學變化材料、潛像花樣等之複製、複印係爲困難而在視覺上可容易地進行真僞認證者，或是壓花加工、附加凹凸、穿孔等之可藉手指感覺或是視覺而進行真僞判別者。

於圖 3，係展示有在日本特開平 10-44650 號公報中所揭示之被安裝有金屬粒所致的人工物特徵辨識・晶片的卡片之先前例子，在此圖中，（a）係爲全體圖，（b）係爲剖面圖，（c）係爲真僞認證晶片的擴大圖。

此卡片 1，係在被形成有識別用之開口 8 而爲光不透過性之卡片基體 7 之上，被層積有混入金屬粒 5 之光透過性樹脂所成的薄板狀之人工物特徵辨識・晶片 4，而在其上，於與被形成在卡片基體 7 上之開口相同的位置，被形成有開口，並被層積有被形成了磁性條 2 與箭頭 3 之不透明的卡片表面板 6。

金屬粒 5，係不具備有任何之規則性，而被混入於 3 維之光透過樹脂中，因此，經由開口所觀測到的金屬粒 5 之配置圖案，係爲各個人工物特徵辨識・晶片 4 所固有者。

利用此事，藉由將透過人工物特徵辨識・晶片 4 之光，經由開口而作攝影，來觀察金屬粒 5 之配置圖案，並識別各個人工物特徵辨識・晶片 4，亦即是識別卡片。

於圖 4，展示在日本特開 2003-29636 號公報所揭示之被安裝有纖維所致的人工物特徵辨識・晶片之真僞識別卡片的其他先前例子。於此圖中，（a）係爲全體圖，（b）係爲剖面圖，（c）係爲人工物特徵辨識・晶片的擴大圖。

此卡片，係在爲光不透過性之卡片基體 1 的開口處，被嵌入有於透明樹脂中將網格構件 9 與短小纖維 10 以 3 維地混入而構成之人工物特徵辨識・晶片 8，而在卡片基體 1 之表面，被形成有磁性條 2 與箭頭 3。在人工物特徵辨識・晶片 8 中，係藉由網格構件 9 之圖案與短小纖維 10 而產生干涉圖案。

此干涉圖案，係爲人工物特徵辨識・晶片 8，亦即是卡片所各別固有者，利用此事，而藉由透過光或是反射光來對真僞認證晶片之人工物特徵辨識・晶片 8 的識別圖案作攝影，以識別卡片。

對於生物特徵辨識或是人工物特徵辨識一般之圖案的機械讀取，一般係經由攝像裝置來讀取，並經由圖案認識

技術來作判別。因此，有藉由複印技術而被僞造的可能。

由於人工物特徵辨識・晶片並不是影像，而是由實體物所構成，因此想要將成爲僞造對象之構成人工物特徵辨識・晶片的要素，以與真正之物相同的形態而配置，係爲不可能。但是，就算僅是偶然，亦無法完全否認經由相同之構成要素而出現相同圖案的可能性，而此種偶然所得到的僞造物，係作爲真正之物而可通用。因此，若是僅經由人工物特徵辨識・晶片來確認卡片等之真正與否，則係爲危險。

如此這般，對卡片本身之真僞作判別的技術係尚未被確立，而無法被僞造之卡片亦尚未被實現。故而，使僞造卡片之使用成爲不可能的技術係尚未被實現。

[專利文獻 1]日本特開平 10-44650 號公報

[專利文獻 2]日本特開平 2003-29636 號公報

[非專利文獻 1]「金融業務與人工物特徵辨識」（日本銀行金融研究所）（http:// www.imes.boj.or.jp/japanese /jdps/2004/04-J-12.pdf）

[非專利文獻 2]「第 6 次資訊安全研討會「金融領域中之人工物特徵辨識」之情況」（http://www.imes.boj.or.jp/japanese/kinyu/2004/kk23-2-6.pdf）[非專利文獻 3]「聯合 IC 卡片卷面之僞造防止技術手冊」，財務省印刷局，（http://www.npb.go.jp /ja/info/ichb.pdf）。

【發明內容】

(12)

〔發明所欲解決之課題〕

在本申請中，係提供一種：不對先前所被汎用之金融卡或是信用卡作基本的變更，而能提高安全性之卡片、卡片處理方法。

本申請之發明，係將在減輕真僞認證作業之負擔的同時，亦能將偶然所得到之僞造物被作爲真正之物而通用的可能性排除一事作爲課題。

〔用以解決課題之手段〕

因此，本申請之發明，係在將使用於卡片之真僞認證而難以僞造的真僞認證晶片作固定接著的同時，在處理卡片之裝置內附加真僞認證裝置。

在真僞認證晶片中係可採用：被分散於透明媒體中之金屬等的粒子、被分散於透明媒體中之纖維片、由被配置於透明媒體中而具備有規則性之圖案與被分散於此透明媒體中之纖維片所致之干涉圖案、壓花全像圖、被分散於透明媒體中之螢光體粒子、被分散於任意之媒體中的放射性物質粒子。

進而，除了真僞認證晶片之外，再設置另一個晶片，而在此晶片中將真僞認證晶片所記載的資訊數位化，並將數位化後之資料加密化，而記載加密化之資料，作爲真僞證明晶片。

在利用卡片時，卡片上之真僞認證晶片的影像係被讀取並被數位化，同時，在同樣之卡片上所附加之真僞證明

晶片的加密化資料係被解碼，而從真僞證明晶片所解碼之資料與真僞認證晶片的加密化資料係被作對照，若是一致，則將此卡片認定爲真正之物，若是不一致，則此卡片係被判斷爲僞造。

在加密金鑰系統中，最簡便的方法，是使用僅有卡片發行者才知道的秘密金鑰，但是亦可以使用在加密化與解碼化中使用相異之金鑰的公開金鑰系統。在公開金鑰系統中，雖係使用公開金鑰與專用金鑰，但是在加密化與解碼化之中，係可使用任一方的金鑰。

爲了減輕加密化／解碼化之負擔，係使用 MD5（Message Digest），SAH-1（Secure Hash Algorithm-1），SAH-2 等之雜湊演算法。

在被數位化之資料內，附加又或是混入卡片等之 ID、持有者之資訊，而將其全體加密化。進而，在被數位化之資料內插入電子浮水印。數位資料之雜湊值化，ID、持有者之資訊的附加，電子浮水印的插入，係僅使用有任一者，或是將數個作組合而使用。

處理卡片之裝置，係在開始密碼之輸入等的具體操作前，先判別卡片的真僞，而決定是將僞造卡片排出、或是發出警報、亦或是將僞造卡片收入至處理裝置內。

〔發明之效果〕

被分散於透明媒體中之金屬等的粒子、被分散於透明媒體中之纖維片、由被配置於透明媒體中而具備有規則性

之圖案與被分散於此透明媒體中之纖維片所致之干涉圖案、被分散於透明媒體中之螢光體粒子、被分散於任意之媒體中的放射性物質粒子，由於係僅爲偶然所得到者，因此複製係爲不可能。又，壓化全像圖由於係具有立體構造，因此除了從原型而直接製造複製品之外，係不可能對其作複製。

又，將磁性記錄資料或是 IC 晶片內之資料作拷貝之僞造卡片，係被排除而使使用成爲不可能。

進而，當欲進行不正當之使用時，其使用係被拒絕，而能防止被害於未然，或者是藉由對不正當之卡片使用作某種程度的許可，並於最終將不正當之卡片作確保，而成爲可以容易地特定出不正當的使用者。

當真僞認證晶片與對其作證明之真僞證明晶片係共存於同一枚之卡片上的情況時，若是將加密金鑰給予至 ATM 等之終端裝置，則不需經過主伺服器，即可確認卡片之真僞。

又，就算是偶然地得到了相同之人工物特徵辨識，並得到了相同的雜湊值，亦由於若是不知道將卡片等之 ID、持有者之資訊等作附加又或是混入的演算法，便無法得知被使用於加密化的加密金鑰，因此安全性係高。

【實施方式】

以下，參考圖面而展示用以實施發明之最佳形態。

首先，針對卡片真僞認證晶片作說明。

〔真偽認證晶片實施例 1〕

於圖 5 所示，係爲作爲真偽認證晶片，而被安裝有壓花全像圖晶片的卡片之基本構成的實施例 1。於此圖中，（a）係爲全體圖，（b）係爲剖面圖，（c）係爲壓花全像圖晶片的擴大圖。

此卡片 11，係在爲不透光性之卡片基體 13 上，被安裝有被形成有開口之表面板 14，而在此開口，被嵌入有壓花全像圖晶片 12。又，在表面板 14 上，係被形成有磁性條 2 與箭頭 3。

壓花全像圖，係由被形成爲所使用之雷射光的 1/4 波長之深度的孔，與未形成有孔之部分而構成，在具有孔的部分，係藉由射出之雷射光與射入之雷射光相互抵消，而使射出之雷射光不會被檢測出，在不具有孔的部分，則射出之雷射光與射入之雷射光不會相互抵消，而使射出之雷射光會被檢測出。

被使用之雷射光，在 CD 的情況係爲 λ = 780nm 之紅外雷射，而 λ /4= 195nm。當 DVD 的情況時，係使用 λ = 650nm 之紅色雷射，而 λ /4= 151.25nm。當次世代 DVD 的情況時，係檢討有使用 μ = 405nm 之藍紫色雷射、λ = 351nm 之紫外雷射、λ = 266nm 之遠紫外雷射，而 λ /4 係各別爲 101.25nm、87.75nm、66.5nm。

於（c）中所示，是最爲基本之構造，在全像圖晶片 15 上，以適當的間隔，被配置有深度爲所使用之雷射光的

1/4 波長之孔 16，以及未被形成有孔之部分 17。於此圖中所示之例的情況，以雙方向箭頭所表示之實線，係顯示其同時具有射入光以及射出光，而以單方向箭頭所表示之虛線，係指雖有射入光但卻沒有射出光。

於（d）中所示，係爲使雷射光之方向傾斜之例，若是沒有傾斜角的資訊，則被寫入之資料的讀取係成爲困難。於此例中，係在全像圖晶片 18 上，以適當的間隔，被配置有深度爲所使用之雷射光的 1/4 波長之傾斜的孔 19，以及未被形成有孔之傾斜部分 20。於此圖中所示之例的情況，以雙方向箭頭所表示之實線，亦係顯示其同時具有射入光以及射出光，而以單方向箭頭所表示之虛線，亦係指雖有射入光但卻沒有射出光。對此構造作複製一事，係近乎不可能。另外，亦可以使（c）中所示之構造與（d）中所示之構造共存。

於（e）中所示，係爲利用有複數之波長的雷射光之例，若是沒有被使用的雷射光之全部的波長資訊，則被寫入之資料的讀取係成爲困難。於此例中，在全像圖晶片 21，係以適當的間隔，被配置有深度爲紅色（R）雷射光之 1/4 波長的孔 22；和深度爲綠色（G）雷射光之 1/4 波長的孔 23；和深度爲藍色（B）雷射光之 1/4 波長的孔 25；和未被形成有孔之部分 24。

於此圖中所示之例的情況，以雙方向箭頭所表示之實線，亦係顯示其同時具有射入光以及射出光，而以單方向箭頭所表示之虛線，亦係指雖有射入光但卻沒有射出光。

對此構造作複製一事，係更近乎於不可能。另外，亦可以使（d）中所示之構造與（e）中所示之構造共存。

〔真僞認證晶片實施例 2〕

於圖 6，係展示真僞認證晶片之實施例 2。於此圖中，（a）係爲由上方俯視卡片之圖，（b）係爲其剖面圖，（c）係爲剖面圖的擴大圖。此卡片 31，係在爲不透光性之卡片基體 35 上，被安裝有被形成有開口之表面板 34，而在此開口，被嵌入有混入螢光物質粒子 33 而構成之真僞認證晶片 32。另外，在真僞認證晶片 32 與表面板 34 之上，係亦可更進而層積有其他的表面板。

卡片基板 35 係爲被使用於在先前被多所使用之金融卡的合成樹脂厚板，或是被使用於預付卡等之合成樹脂薄板。真僞認證晶片 32，係具備有嵌合於表面板 34 之開口的面積以及厚度，而被混入有螢光物質粒子 33。

表面板 35 之材料，係可使用相對於卡片之射入光及射出光係爲透明之合成樹脂，或是相對於卡片之射入光以及／又或是射出光係爲不透明，而相對於其他之可視光線係爲不透明的合成樹脂之任一者。另外，在以合成樹脂所構成之真僞認證晶片 32 與表面板 34 之上所進而層積之表面板，係使用相對於射入光以及射出光係爲透明的合成樹脂。

〔真僞認證晶片實施例 3〕

於圖 7，係展示真偽認證晶片之實施例 3。於此圖中，（a）係爲由上方俯視卡片之圖，（b）係爲其剖面圖，（c）係爲剖面圖的擴大圖。此卡片 41，係在爲不透光性之卡片基體 45 上，被安裝有被形成有開口之表面板 44，而在此開口，被嵌入有於樹脂中混入放射性物質粒子 20 而構成之真偽認證晶片 42。又，在表面板 44 上，係被形成有磁性條 2 與箭頭 3。

此被混入之放射性物質粒子的配置圖案，係爲此真偽認證晶片 42，亦即是卡片 41 所固有之物，而利用此事，來對卡片作識別。

〔真偽認證晶片安裝位置實施例 1〕

於圖 8，係展示具備有此些構造之真偽認證晶片的被安裝於卡片之安裝位置的實施例。真偽認證晶片 46 之安裝位置，係除了在圖 5～圖 7 所示之卡片本體的幾乎中央之位置以外，係可安裝於圖 8（a）所示之中段前端位置、（b）所示之中段中央位置，另外，亦可安裝於（c）所示之中段後端位置、（d）所示之下段前端位置、（e）所示之下段中央位置、（f）所示之下段後端位置。上段位置雖亦爲可能，但是在有可能會對從磁性條之資訊的讀取造成影響的情況時，係以避免將其配置在上段位置爲理想。

〔真偽認證晶片安裝位置實施例 2〕

從卡片之安全性強化、或是便利化強化的觀點而言，

98年11月25日修正替換頁

於資訊記憶媒體使用 IC 晶片一事係在進行。此 IC 晶片係在內部具備有半導體記憶體，而若是此半導體記憶體被輻射線、特別是被身爲電子線之 β 線所照射，則會有記憶體被抹寫的情況。

在輻射線之中，由於 α 線係只要以一張紙即可遮蔽，因此幾乎不需要考慮其對半導體記憶體的影響。但是，若要遮蔽 β 線，則至少需要 1mm 厚的鋁板，或是 10mm 厚的丙烯樹脂板。因此，在使用輻射出 β 線的輻射性物質粒子時，係如圖 9（a）、（c）、（d）、以及（f）所示，藉由將真僞認證晶片 46 與 IC 晶片 47 之間相離 10mm 以上之間隔而配置，而能避免 β 線所造成之影響。

〔真僞認證晶片讀取位置〕

金融卡以及信用卡之物理上的規格，從汎用性的觀點來看，係被嚴格規定，因此被設置於其上者，其物理規格自然亦係爲嚴格。但是，亦無法否定由於過酷的使用而使其產生變形的可能性。

爲了預防此種情況，係以在真僞認證晶片中，形成於圖 10 所示之位置對準用記號 48 爲理想。位置對準用記號，在最單純的情況，係爲 1 個亦可，但是爲了更確實地進行位置對準，係設置有複數個。

爲了更確實地進行讀取，因此與位置對準用記號兼用，而在真僞認證晶片之讀取開始位置以及讀取結束位置，設置某些之記號，例如如圖 10 所示之移動方向讀取開始

線 49 以及移動方向讀取結束線 50，並更進而設置端部指示線 51、52。

真偽認證晶片上之資訊的讀取，由於係藉由真偽認證晶片與讀取裝置之相對運動而進行，因此爲了確實地進行讀取，有必要將真偽認證晶片與讀取裝置之運動作同步。故而，只要在真偽認證晶片上形成同步訊號用之記號 87，即可在記號之讀取中使讀取裝置之運動與其同步。

亦可將讀取開始・結束線以及／又或是同步訊號用之記號，利用於訊號處理時之訊號正規化。此些之位置對準用記號、讀取開始・結束線以及／又或是同步訊號用之記號，係任一均爲由螢光體所構成，而可藉由例如噴墨印表機一般之適當的印刷手段而形成。

〔真偽認證晶片實施例 4〕

於圖 6～圖 7 所示之卡片真偽認證晶片，係爲人工物特徵辨識。將人工特徵辨識物作僞造一事係爲不可能，但是相反地，在製造時，對圖案作控制一事亦爲不可能。藉由圖 11～圖 20，展示身爲適合於機械之讀取的 2 值資料之經由電腦所作成的真偽認證晶片之構成例。

於圖 11 所示之真偽認證晶片，係將 1024 個的 2 值資料配置於 32x32 的矩陣中，於此圖，被寫入有 2 值資料「0」之場所，係以空白來顯示，而被寫入有 2 值資料「1」之場所，則係以「＊」來顯示。

針對得到此 2 值資料的方法作說明。於圖 12 所示，

係爲經由檢測出藉輻射性物質之核崩壞所輻射出的輻射線，所得到之16進位數256位數的真性亂數的實例，被使用於加密金鑰的亂數，通常係如此這般作爲16進位數而被供給。於圖13，係展示將圖12所示之16進位亂數配列於8列32行之矩陣者。

此16進位數，係可置換爲4位的2進位數而表現之。亦即是，16進位數之「0」係爲2進位數之「0000」，同樣的，「1」係爲「0001」，「2」係爲「0010」、「3」係爲「0011」、「4」係爲「0100」、「5」係爲「0101」、「6」係爲「0110」、「7」係爲「0111」、「8」係爲「1000」、「9」係爲「1001」、「A」係爲「1010」、「B」係爲「1011」、「C」係爲「1100」、「D」係爲「1101」、「E」係爲「1110」、「F」係爲「1111」，而各自被表現。

根據此，而將圖12所示之256位數的16進位亂數置換爲2進位亂數者，係成爲如圖14所示。由於1位數的16進位數係被置換爲4位數的2進位數，因此256位數的16進位數係被置換爲256位數×4位數＝1024位數的2進位數。此些之2進位數，由於係爲在亂數裝置中可直接得到者，因此在此情況，置換之操作係爲不必要。

將此配列爲如圖13所示之8列32行的矩陣，並進而於圖15展示將2進位數之位數單位配列爲32列32行的矩陣者。

最後，藉由在圖15中的矩陣中之相當於2進位數的0

之處不寫入任何資訊而保持原狀態，並在相當於 1 之被顯示爲「＊」處將資訊寫入，而能得到如圖 11 所示之真僞認證晶片的配列。如此這般所形成之真僞認證晶片，係具備有 32 列x32 行x1 位元＝1024 位元之真僞判別資訊，亦即是 1024 位元之真僞判別金鑰。

於圖 5（c）所示之壓花全像圖，以及圖 6 所示之螢光物質，係可使用複數波長之光。接下來，展示身爲 2 値資料，並適合於機械讀取，經由電腦所作成，而利用一般之紅（R）、綠（G）、藍（B）的光之卡片真僞認證晶片的位元構成例。

此些之「R」、「G」、「B」，係亦包含未寫入資料之狀態的「0」，而可表現 4 種之狀態。換言之，可將此些當成 4 進位數而處理，4 進位數，係可藉由 4 個的 2 位元數，也就是「00」、「01」、「10」、「11」來表現。

於圖 16 所示，係爲將圖 12 所示之 256 位數的 16 進位亂數之前端，更進而合併 256 位數之 16 進位亂數而表示者。於此，「16 進位亂數列 a」係爲和圖 12 所示者相同之亂數列，而「16 進位亂數 b」則係爲置於「16 進位亂數列 a」之前端的亂數列。

於圖 17，係展示將此 16 進位亂數列變換爲 2 進位亂數列後，爲了將其轉換爲以 0、R、G、所表現的 4 進位數，而於每 2 個位元作區隔後的亂數列。

進而，於圖 18，係展示將 2 進位數「00」轉換爲 4 進位數「0」，將 2 進位數「01」轉換爲 4 進位數「R」，將

2進位數「10」轉換爲4進位數「G」，而將2進位數「11」轉換爲4進位數「B」者。

於圖19，係展示將如此這般所得到之4進位數，和圖11或是圖15所示之2進位數同樣地配列於32列32行之矩陣者。如此這般所形成之真僞認證晶片，係具備有32列×32行×2位元＝2048位元之真僞認證資訊，亦即是2048位元之真僞認證金鑰。

藉由圖20，說明從1個的亂數列得到複數之真僞判別晶片的方法。於此圖中，（a）、（b）、（c）、（d）係各別爲根據圖11所示之32×32的矩陣圖案而得到16×16之矩陣圖案者，（a）係以座標（0，0）爲原點，（b）係以座標（1，0）爲原點，（c）係以座標（0，1）爲原點，而（d）係以座標（1，1）爲起點。

如此這般，能從由圖12中所示之亂數列所得到的1個的矩陣圖案，而得到複數之矩陣圖案。

爲了從1個亂數列得到複數之矩陣圖案，除了上述方法之外，亦可利用各種之方法，例如使圖12所示之亂數列的使用開始位置變化，或是使圖13所示之矩陣圖案的作成開始位置變化等。

藉由如此進行，卡片發行者係成爲可將1個的亂數列作爲主亂數列而秘密地保管，而根據此主亂數列來得到複數之矩陣圖案。又，複數之矩陣圖案，係經由原點的資訊而可自動管理。

於圖11及圖15所示之實施例，係藉由以1位元來表

現之 2 進位數來記錄真僞認證資訊，而圖 19 所示之實施例，則係藉由以 2 位元來表現之 4 進位數來記錄真僞認證資訊。作爲此些之延長，亦可使用以 3 位元來表現的 8 進位數，以及以 4 位元來表現的 16 進位數。

〔證明晶片實施例 1〕

於圖 21 以及圖 22，展示對卡片本身作證明之卡片的實施例。於圖 21 係展示卡片，而於圖 22 係展示真僞認證晶片以及真僞證明晶片之功能。

在卡片 60 中，係以不可與卡片本體分離之構造，而被安裝有：真僞認證資訊晶片 61，其係收容有人工物特徵辨識等之卡片真僞認證資訊「A」（Authentication）；和真僞證明晶片 62，其係收容有將真僞認證資訊「A」之數位化資料「M」（Message）加密化後之加密化資料「C」。又，在卡片 60 之表面的上部，係被形成有磁性條 2 與箭頭 3。

亦可將 IC 晶片代替磁性條 2，或是與磁性條 2 共同使用。又，真僞認證晶片 61 與真僞證明晶片 62，雖亦可如圖 21 所示，分別配置在不同之位置，但是亦可使其鄰接或是一體化的配置。

藉由圖 22，針對於圖 21 所示之卡片 60 上的真僞認證晶片 61 與真僞證明晶片 62 的功能，說明基本的實施例。於此圖中，（1）～（5）係爲針對卡片發行者作成卡片時之時的說明，而（6）～（10）係爲針對利用者使用 ATM

等之終端裝置而利用卡片之時的說明。

（1）作成收容有身爲人工物特徵辨識或是壓花全像圖之卡片真僞認證資訊「A」的真僞認證晶片 61。由於各別之人工物特徵辨識係全部爲相異，因此具備有人工物特徵辨識之真僞認證晶片 61 係全部爲相異。

又，只要藉由圖 11～圖 20 所示之方法，並使用 32 位元×32 位元＝1024 位元（10 進位數而 307 位數）之資料又或是更多的位元數之資料，來作成圖 5～圖 7 所示之真僞認證晶片，則存在有相同之真僞認證晶片的確率，係降低至極小而可以忽視。又，由於壓花全像圖係具備有 3 維之構造，因此光學之複製係爲不可能，而在僞造上係極爲困難。

（2）將真僞認證晶片 61 之資訊，類比地又或是數位地讀取。爲了能正確地進行利用卡片時之讀取，係以將真僞認證晶片 61 安裝於卡片 60 上之後再進行讀取爲理想。

（3）將被讀取後之真僞認證晶片 61 之類比影像，數位化成數位資料「M」。另外，當被讀取之收容於真僞認證晶片 61 的資料係爲數位資料時，則不需要作數位化。

（4）將數位資料「M」加密化，而得到加密化資料「C」。作爲加密化系統，可利用秘密金鑰加密系統（Secret-key Cryptosystem）、公開金鑰加密系統（Public-key Cryptosystem）。

在秘密金鑰加密系統（Secret-key Cryptosystem）中所使用的加密金鑰，雖被稱爲秘密金鑰（Secret-key），

98年11月25日修正替換頁

但是近年來由於隨著公開金鑰加密系統之普及，將公開金鑰加密系統中所使用之專用金鑰（Public-key）稱爲秘密金鑰（Secret-key）的人亦逐漸增加，因此爲了避免混淆，亦有將其稱爲共通金鑰（Common-key）的情況。

若是依據電子資訊通訊學會刊「現代加密理論」，則係將使用加密金鑰 K（Key）來將訊息 M（Message）加密化而得到加密化資料（enCrypted-data）之過程，表示爲 C＝E（K，M），將使用加密金鑰而將加密化資料 C 解碼化（Decryption）而得到解碼化資料之過程，表現爲 M＝D（K，C）。

於此，係仿照上述，將使用秘密金鑰加密系統之秘密金鑰 Ks 來將數位資料「M」加密化而得到加密化資料「Cs」之過程，表示爲 Cs＝E（Ks，M），將使用秘密金鑰 Ks 而將加密化資料「Cs」解碼化而得到數位化資料「M」之過程，表現爲 M＝D（Ks，Cs）。

將使用公開金鑰加密系統之公開金鑰 Kp 來將數位資料「M」加密化而得到加密化資料「Cp」之過程，表示爲 Cp＝E（Kp，M），將使用專用金鑰 Kv 而將加密化資料「Cp」解碼化而得到數位・影像・資料「M」之過程，表現爲 M＝D（Kv，Cp）。加密金鑰之配送，係如此這般而進行。

將使用公開金鑰加密系統之專用金鑰 Kv 來將數位資料「M」加密化而得到加密化資料 Cv 之過程，表示爲 Cv＝E（Kv，M），將使用公開金鑰 Kp 而將加密化資料「Cv

98年11月25日修正替換頁

」解碼化而得到數位化資料「M」之過程，表現爲 M＝D（Kp，Cv）。數位署名，係如此這般而進行。

（5）將加密化資料「Cs」、「Cp」又或是 Cv」，記錄・保存於證明晶片 62 中，並將證明晶片以不可與卡片本體 60 分離的構造來安裝。在暗號資料之記錄・保存中，係可採用條碼、2 維條碼等之光學式讀取記錄方法，磁性記錄等適當者。

當卡片 60 係爲搭載有 IC 晶片之 IC 卡片的情況時，亦可將加密化資料收容於 IC 晶片內。此時，係採用不可分離之構造的一體構造，或是採用溶著等之方法。又，亦可不將晶片安裝於卡片，而將加密化資料記錄在卡片本身之中。

（6）在利用卡片時，係從真僞證明晶片 62 中，讀取出所收容之加密化資料「C」。

（7）使用特定之暗號演算法以及加密金鑰，而將加密化資料「C」解碼化，而得到解碼化資料「M」。

（8）同時，讀取出真僞認證晶片 61 之資訊「A'」。讀取手段，最一般的係爲使用攝像機，但是亦可使用攝像機以外的讀取頭或是掃瞄機等。

（9）將被讀取後之認證晶片的資訊「A'」數位化，而得到數位資料「M'」。

（10）將被解碼之資料「M」與被數位化後之資料「M'」作比較。若兩者係爲同一，則判斷真僞認證晶片 61 與真僞證明晶片 62 之組合係爲正當，若是相異，則判斷

真偽認證晶片 61 與真偽證明晶片 62 之組合係爲不正當，並判斷卡片係爲不正當。如此這般，真偽認證晶片 61 之正當性，係經由共同存在於卡片上之真偽證明晶片 62 而被證明。

在此實施例中，雖係將由真偽認證晶片 61 所讀取之資料「M'」與從真偽證明晶片 62 所解碼化之資料「M」作比較，但是，亦可構成爲：對將從真偽認證晶片 61 所讀取之資料「M'」加密化後之加密化資料「C'」與從真偽證明晶片 62 所讀取之加密化資料「C」作比較。

真偽證明晶片 62 之資料，係被加密化。此加密系統，係可採用使用單一之加密金鑰的秘密金鑰（或是共通金鑰）加密系統，以及使用 2 個加密金鑰的公開金鑰方式中之任一者。在公開金鑰系統中，使用於加密化以及解碼化之金鑰，係亦可採用公開金鑰與專用金鑰（秘密金鑰）之組合或是專用金鑰與公開金鑰之組合的任一組合。

當利用者經由終端裝置而利用卡片時，雖係使用解碼化用之加密金鑰，但是作爲加密金鑰之保管場所，係爲在伺服器內以及終端裝置內。若是構成爲將加密金鑰保管於伺服器內，並在每次之有必要作卡片之真偽認證時，將必要的加密金鑰配信於終端裝置，則能夠成爲線上之安全性高的方法。若是加密金鑰被保管在終端裝置內，則卡片之真偽認證係可在離線狀態僅經由終端裝置而進行。但是，若是終端裝置遭到竊取，則加密金鑰亦成爲被盜取。爲了防止此種事態，若是構成爲：將加密金鑰保管於終端裝置

內之 DRAM，並在終端裝置因遭到破壞或是竊取使電源被切斷時，使被保管於 DRAM 中之加密金鑰成爲消失，則能防止加密金鑰之被盜取。

〔證明晶片實施例 2〕

當將用以確認卡片之真僞而被保存的資料，從主伺服器送訊至終端裝置，而在終端裝置側對真僞作認證，或者是將讀取之卡片的資料送訊至伺服器側而在伺服器側作認證的情況時，由於從真僞認證晶片 61 而來之數位資料係爲大，因此伺服器之保存資料量以及通訊資料量係變大。

作爲其對策，舉例而言，若是使用身爲代表性之雜湊演算法的 MD5（Message Digest 5）、SAH-1（Secure Hash Algorithm-1）、SAH-2 等之雜湊演算法，則不論是再大的資料，亦可變換爲 16 位元之雜湊值，且對原本之資料所做的改寫必定會反映在雜湊值中。若是利用此，則能不使伺服器之保存資料量以及通訊資料量變大。爲了減輕加密化／解碼化之負擔，係使用雜湊演算法。

於圖 23 以及圖 24，展示使用有雜湊演算法之卡片的實施例。於圖 23 係展示卡片，而於圖 24 係展示真僞認證晶片以及真僞認證晶片之功能。

此卡片 63，係以不可與卡片本體分離之構造，而被安裝有：真僞認證資訊晶片 61，其係收容有人工物特徵辨識等之卡片真僞認證資訊「A」（Authentication）；和真僞證明晶片 64，其係將真僞認證資訊「A」之數位化資料「

M」（Message）雜湊值化並作爲雜湊值「H」，並將雜湊值「H」加密化而作爲加密化資料「Ch」，而收容加密化資料「Ch」。又，在卡片 63 之表面的上部，係被形成有磁性條 2 與箭頭 3。亦可將 IC 晶片代替磁性條 2，或是與磁性條 2 共同使用。又，真僞認證晶片 61 與真僞證明晶片 64，雖亦可如圖 23 所示，分別配置在不同之位置，但是亦可使其鄰接或是一體化的配置。

藉由圖 24，針對於圖 23 所示之卡片 63 上的真僞認證晶片 61 與真僞證明晶片 64 的功能作說明。於此圖中，（1）～（6）係爲針對卡片發行者作成卡片時的說明，而（7）～（11）係爲針對利用者使用 ATM 等之終端裝置而利用卡片時的說明。

（1）作成收容有身爲人工物特徵辨識或是壓花全像圖之卡片真僞認證資訊「A」的真僞認證晶片 61，由於各別之人工物特徵辨識係全部爲相異，因此具備有人工物特徵辨識之真僞認證晶片 61 係全部爲相異。特別是，由於具備有 3 維配置之人工物特徵辨識的複製係爲不可能，因此係無法被僞造。

又，只要藉由圖 11～圖 20 所示之方法，並使用 32 位元x32 位元＝1024 位元（10 進位數而 307 位數）之資料又或是更多的位元數之資料，來作成圖 5～圖 7 所示之真僞認證晶片，則存在有相同之真僞認證晶片的確率，係降低至極小而可以忽視。又，由於壓花全像圖係具備有 3 維之構造，因此光學之複製係爲不可能，而在僞造上係極爲困

難。

（2）將真偽認證晶片 61 之資訊，類比地又或是數位地讀取。爲了能正確地進行利用卡片時之讀取，係以將真偽認證晶片 61 安裝於卡片 63 上之後再進行讀取爲理想。

（3）將被讀取後之真偽認證晶片 61 之類比影像，數位化成數位資料「M」。另外，當被讀取之收容於真偽認證晶片 61 的資料係爲數位資料時，則不需要作數位化。

（4）將數位資料「M」雜湊值化，而得到雜湊值「H」。藉由汎用之 MD5 演算法所得之雜湊值，或是其他情況所得之雜湊值，係爲 16 位元組（＝128 位元）。

（5）將雜湊值「H」加密化，而得到加密化資料「Ch」。作爲加密化系統，可利用秘密金鑰加密系統（Secret-key Cryptosystem）、公開金鑰加密系統（Public-key Cryptosystem）。

（6）將加密化資料「Ch」，記錄・保存於真偽證明晶片 64 中，並將證明晶片以不可與卡片本體 63 分離的構造來安裝。在暗號資料之記錄・保存中，係可採用條碼、2 維條碼等之光學式讀取記錄方法，磁性記錄等適當者。

當卡片 63 係爲搭載有 IC 晶片之 IC 卡片的情況時，亦可將加密化資料收容於 IC 晶片內。此時，係採用不可分離之構造的一體構造，或是採用溶著等之方法。又，亦可不安裝晶片，而將加密化資料記錄在卡片本身之中。

（7）在利用卡片時，係從真偽證明晶片 64 中，讀取出所收容之加密化資料「Ch」。

（8）使用特定之暗號演算法以及加密金鑰，而將加密化資料「Ch」解碼化，而得到解碼化資料「H」。

（9）同時，讀取出真僞認證晶片 61 之資訊「A'」。讀取手段，最一般的係爲使用攝像機，但是亦可使用攝像機以外的讀取頭或是掃瞄機等。

（10）將被讀取後之認證晶片的資訊「A'」數位化，而得到數位資料「M'」。

（11）將數位資料「M'」雜湊值化，而得到雜湊值「H'」。

（12）將解碼化之資料「H」與雜湊值「H'」作比較。

若兩者係爲同一，則判斷真僞認證晶片 61 與真僞證明晶片 64 之組合係爲正當，若是相異，則判斷真僞認證晶片 61 與真僞證明晶片 64 之組合係爲不正當，並判斷卡片係爲不正當。如此這般，真僞認證晶片 61 之正當性，係經由與真僞認證晶片 61 共同存在於卡片上之真僞證明晶片 64 而被證明。

在此實施例中，雖係爲將由真僞認證晶片 61 所讀取之資料「M'」雜湊值化後之雜湊值「H'」，與將從真僞證明晶片 64 所讀取之加密化雜湊值「Ch」所解碼之雜湊值「H」作比較，但是，亦可相反地構成爲：對將從真僞認證晶片 61 所讀取之資料「M'」雜湊值化後之雜湊值「H'」加密化，並將加密化後之加密化雜湊值「Ch'」與從真僞證明晶片 64 所讀取之加密化資料「Ch」作比較。

98年11月25日修正替換頁

另外，在此實施例中所使用之加密系統、加密金鑰之使用法及管理方法，由於相較於證明晶片之實施例 1 的情況係並未改變，因此係省略其說明。

〔證明晶片實施例 3〕

認證晶片，係有可能因爲破損或是污損，而使得認證資訊之讀取變爲不可能的情形。如此一來，就算此卡片係爲正當者，亦成爲無法使用。說明用以對應此種事態之構成。

於圖 25 以及圖 26，展示使用卡片之 ID 的卡片之實施例。於圖 25 係展示卡片，而於圖 26 係展示圖 25 所示之真僞認證晶片以及真僞證明晶片之功能。

此卡片 65，係以不可與卡片本體分離之構造，而被安裝有：真僞認證資訊晶片 61，其係收容有人工物特徵辨識等之卡片真僞認證資訊「A」（Authentication）；和真僞證明晶片 66，其係在真僞認證資訊「A」之數位化資料「M」（Message）附加有卡片之 ID 等的資訊並作爲 ID 附加資料「I」，並將 ID 附加資料「I」加密化而作爲加密化資料「Ci」，而收容加密化資料「Ci」。又，在卡片 65 之表面的上部，係被形成有磁性條 2 與箭頭 3。亦可將 IC 晶片代替磁性條 2，或是與磁性條 2 共同使用。又，真僞認證晶片 61 與真僞證明晶片 66，雖亦可如圖 25 所示，分別配置在不同之位置，但是亦可使其鄰接或是一體化的配置。

藉由圖 26，針對於圖 25 所示之卡片 65 上的真僞認證晶片 61 與真僞證明晶片 66 的功能作說明。於此圖中，（1）～（6）係爲針對卡片發行者作成卡片時的說明，而（7）～（11）係爲針對利用者使用 ATM 等之終端裝置而利用卡片時的說明。

（1）作成收容有身爲人工物特徵辨識或是壓花全像圖之卡片真僞認證資訊「A」的真僞認證晶片 61。

由於各別之人工物特徵辨識係全部爲相異，因此具備有人工物特徵辨識之真僞認證晶片 61 係全部爲相異。特別是，由於具備有 3 維配置之人工物特徵辨識的複製係爲不可能，因此係無法被僞造。

又，只要藉由圖 11～圖 20 所示之方法，並使用 32 位元x32 位元＝1024 位元（10 進位數而 307 位數）之資料又或是更多的位元數之資料，來作成圖 5～圖 7 所示之真僞認證晶片，則存在有相同之真僞認證晶片的確率，係降低至極小而可以忽視。又，由於壓花全像圖係具備有 3 維之構造，因此光學之複製係爲不可能，而在僞造上係極爲困難。

（2）將真僞認證晶片 61 之資訊，類比地又或是數位地讀取。爲了能正確地進行利用卡片時之讀取，係以將真僞認證晶片 61 安裝於卡片 65 上之後再進行讀取爲理想。

（3）將被讀取後之真僞認證晶片 61 之類比影像，數位化成數位資料「M」。另外，當被讀取之收容於真僞認證晶片 61 的資料係爲數位資料時，則不需要作數位化。

（4）在數位資料「M」中附加卡片之 ID 等的資料，而得到 ID 附加資料「I」。

（5）將 ID 附加資料「I」加密化，而得到加密化資料「Ci」。作爲加密化系統，可利用秘密金鑰加密系統（Secret-key Cryptosystem）、公開金鑰加密系統（Public-key Cryptosystem）。

（6）將加密化資料「Ci」，記錄・保存於真僞證明晶片 66 中，並將證明晶片以不可與卡片本體 65 分離的構造來安裝。在暗號資料之記錄・保存中，係可採用條碼、2 維條碼等之光學式讀取記錄方法，磁性記錄等適當者。

當卡片 65 係爲搭載有 IC 晶片之 IC 卡片的情況時，亦可將加密化資料收容於 IC 晶片內。此時，係採用不可分離之構造的一體構造，或是採用溶著等之方法。又，亦可不安裝晶片，而將加密化資料記錄在卡片本身之中。

（7）在利用卡片時，係從真僞證明晶片 66 中，讀取出所收容之加密化資料「Ci」。

（8）使用特定之暗號演算法以及加密金鑰，而將加密化資料「Ci」解碼化，而得到解碼化資料「I」。

（9）同時，讀取出真僞認證晶片 61 之資訊「A'」。讀取手段，最一般的係爲使用攝像機，但是亦可使用攝像機以外的讀取頭或是掃瞄機等。

（10）將被讀取後之真僞認證晶片 61 的資訊「A'」數位化，而得到數位資料「M'」。

（11）在數位資料「M'」中附加卡片之 ID 等的資料

，而得到ID附加資料「I'」。

（12）將解碼化之資料「I」與ID附加資料「I'」作比較。

若兩者係爲同一，則判斷真僞認證晶片61與真僞證明晶片66之組合係爲正當，若是相異，則判斷真僞認證晶片61與真僞證明晶片66之組合係爲不正當，並判斷卡片係爲不正當。

如此這般，真僞認證晶片61之正當性，係經由共同存在於卡片上之真僞證明晶片66而被證明。

被記錄於真僞證明晶片66之資料，係爲將根據真僞認證晶片61之資訊而於資料中附加有ID的資料作加密化之後所得者。爲了確認真僞認證晶片61之正當性，係有必要在對資料作比較前，將ID附加於從真僞認證晶片66所得到的資料中。藉由將此ID作爲秘密，不知道ID的人，係不可能進行加密解讀而得知加密金鑰。

在此實施例中，係將由真僞認證晶片61所讀取之資訊「A'」數位化而作爲數位資料「M'」，並與附加有卡片資訊之資料「I'」以及將從真僞認證晶片66所讀取之加密化資料「Ci」解碼化後之資料「I」作比較。而，亦可將此相反地構成爲：將由真僞證明晶片66所讀取之資料「Ci」解碼化後之資料「I」除去卡片資訊所得到的數位資料「M」，和將從真僞認證晶片61所讀取之資訊「A'」數位化後所得之數位資料「M'」作比較。

另外，在此實施例中所使用之加密系統、加密金鑰之

使用法及管理方法，由於相較於證明晶片之實施例 1 的情況係並未改變，因此係省略其說明。

真僞認證晶片與真僞證明晶片所共存之卡片，係由利用者來管理。又，在真僞認證晶片中，成爲加密化之對象的真僞認證資訊係以未保護的狀態存在，而在真僞證明晶片中係存在有真僞認證資訊的加密化資料。在此種狀況下，當卡片落入懷有惡意之持有者手中時，或者是利用者本身係爲懷有惡意者時，加密會被解讀，而加密金鑰會被得知。在此說明用以防止此種事態之構成。

於圖 27 以及圖 28，展示使用有電子浮水印之卡片的實施例。於圖 27 係展示卡片，而於圖 28 係展示圖 27 所示之真僞認證晶片以及真僞證明晶片之功能。

此卡片 67，係以不可與卡片本體分離之構造，而被安裝有：真僞認證資訊晶片 61，其係收容有人工物特徵辨識等之卡片真僞認證資訊「A」（Authentication）；和真僞證明晶片 68，其係在真僞認證資訊「A」之數位化資料「M」（Message）附加有電子浮水印並作爲電子浮水印附加資料「W」，並將電子浮水印附加資料「W」加密化而作爲加密化資料「Cw」，而收容加密化資料「Cw」。又，在卡片 67 之表面的上部，係被形成有磁性條 2 與箭頭 3。亦可將 IC 晶片代替磁性條 2，或是與磁性條 2 共同使用。又，真僞認證晶片 61 與真僞證明晶片 68，雖亦可如圖 27 所示，分別配置在不同之位置，但是亦可使其鄰接或是一體化的配置。

(38)

藉由圖 28，針對於圖 27 所示之卡片 67 上的真僞認證晶片 61 與真僞證明晶片 68 的功能作說明。於此圖中，（1）～（6）係爲針對卡片發行者作成卡片時的說明，而（7）～（11）係爲針對利用者使用 ATM 等之終端裝置而利用卡片時的說明。

（1）作成收容有身爲人工物特徵辨識或是壓花全像圖之卡片真僞認證資訊「A」的真僞認證晶片 61。

由於各別之人工物特徵辨識係全部爲相異，因此具備有人工物特徵辨識之真僞認證晶片 61 係全部爲相異。特別是，由於具備有 3 維配置之人工物特徵辨識的複製係爲不可能，因此係無法被僞造。又，只要藉由圖 11～圖 20 所示之方法，並使用 32 位元x32 位元＝1024 位元（10 進位數而 307 位數）之資料又或是更多的位元數之資料，來作成圖 5～圖 7 所示之真僞認證晶片，則存在有相同之真僞認證晶片的確率，係降低至極小而可以忽視。又，由於壓花全像圖係具備有 3 維之構造，因此光學之複製係爲不可能，而在僞造上係極爲困難。

（2）將真僞認證晶片 61 之資訊，類比地又或是數位地讀取。爲了能正確地進行利用卡片時之讀取，係以將真僞認證晶片 61 安裝於卡片 67 上之後再進行讀取爲理想。

（3）將被讀取後之真僞認證晶片 61 之類比影像，數位化成數位資料「M」。另外，當被讀取之收容於真僞認證晶片 61 的資料係爲數位資料時，則不需要作數位化。

（4）於數位資料「M」附加電子浮水印，而得到電子

浮水印附加資料「W」。

（5）將電子浮水印附加資料「W」加密化，而得到加密化資料「Cw」。

（6）將加密化資料「Cw」，記錄・保存於真僞證明晶片68中，並將證明晶片以不可與卡片本體67分離的構造來安裝。在加密化資料之記錄・保存中，係可採用條碼、2維條碼等之光學式讀取記錄方法，磁性記錄等適當者。

當卡片67係爲搭載有IC晶片之IC卡片的情況時，亦可將加密化資料收容於IC晶片內。此時，係採用不可分離之構造的一體構造，或是採用溶著等之方法。又，亦可不安裝晶片，而將加密化資料記錄在卡片本身之中。

（7）在利用卡片時，係從真僞證明晶片68中，讀取出所收容之加密化資料「Cw」。

（8）使用特定之加密演算法以及加密金鑰，而將加密化資料「Cw」解碼化，而得到解碼化資料「W」。

（9）同時，讀取出真僞認證晶片61之資訊「A'」。讀取手段，最一般的係爲使用攝像機，但是亦可使用攝像機以外的讀取頭或是掃瞄機等。

（10）將被讀取後之真僞認證晶片的資訊「A'」數位化，而得到數位資料「M'」。

（11）於數位資料「M'」附加電子浮水印，而得到電子浮水印附加資料「W'」。

將解碼化資料「W」與電子浮水印附加數位資料「W'

98年11月25日修正替換頁

」作比較。若兩者係爲同一，則判斷真僞認證晶片 61 與真僞證明晶片 68 之組合係爲正當，若是相異，則判斷真僞認證晶片 61 與真僞證明晶片 68 之組合係爲不正當。

如此這般，真僞認證晶片 61 之正當性，係經由共同存在於卡片上之真僞證明晶片 68 而被證明。

被記錄於真僞證明晶片 68 之資料，係爲將根據真僞認證晶片 61 之資訊而於資料中附加有電子浮水印的資料作加密化之後所得者。爲了確認真僞認證晶片 61 之正當性，係有必要在對資料作比較前，將電子浮水印附加於從真僞認證晶片 61 所得到的資料中。藉由將此電子浮水印作爲秘密，不知道電子浮水印的人，係不可能進行加密解讀而得知加密金鑰。

在此實施例中，係將由真僞認證晶片 61 所讀取之資訊「A'」數位化而作爲數位資料「M'」，並與附加有電子浮水印之資料「W'」以及將從真僞認證晶片 68 所讀取之加密化資料「Cw」解碼化後之資料「W」作比較。而，亦可將此相反地構成爲：將由真僞證明晶片 68 所讀取之資料「Cw」解碼化後之資料「W」除去電子浮水印所得到的數位資料「M」，和將從真僞認證晶片 61 所讀取之資訊「A'」數位化後所得之數位資料「M'」作比較。

另外，在此實施例中所使用之加密系統、加密金鑰之使用法及管理方法，由於相較於證明晶片之實施例 1 的情況係並未改變，因此係省略其說明。

〔證明晶片實施例 5〕

以上所說明之證明晶片例，係經由在如證明晶片之實施例 1 中所示之基本的構成中，分別追加：雜湊值演算法（實施例 2）、卡片之 ID（實施例 3）、電子浮水印（實施例 4），而使僞造變爲困難。

而此些之被附加的技術，係並不僅是將其單獨附加，而亦可將數個作組合，亦即是，可作：雜湊演算法與卡片等之 ID 的組合；雜湊演算法與電子浮水印的組合；卡片等之 ID 與電子浮水印的組合；或是進而作雜湊演算法與卡片等之 ID 以及電子浮水印的組合。

說明卡片真僞認證的處理流程。

〔處理實施例 1〕

藉由圖 29，說明卡片真僞認證處理流程之實施例 1。

（1）若是卡片之持有者將箭頭部作爲前端而將金融卡插入 ATM 等之終端裝置的卡片插入口內，則卡片插入口之感測器係感測有此，而將卡片取入至裝置內。

（2）當取入卡片時，終端裝置係從卡片之磁性記錄部而讀取卡片資訊。

（3）終端裝置，係判斷被插入之卡片是否爲此終端裝置所能處理的卡片。

（4）當從所讀取之卡片資訊中，無法確認有顯示此卡片係爲可處理的資訊的情況，又或是雖然係爲正當之卡片，卻因爲破損又或是污損等而造成無法讀取出卡片之資

訊時，則終端裝置係將此卡片作爲無法處理之不適當卡片而排出之。

（5）終端裝置，係利用在取入卡片時之卡片的移動而作機械掃瞄，或是在卡片被取入並停止的狀態下，從真僞認證晶片讀取出真僞認證資訊。

（6）終端裝置，係判斷被讀取之卡片真僞認證資訊是否爲正確。

（7）當終端裝置判斷卡片真僞認證資訊係爲不正確時，係將被插入之卡片判斷爲非正規者，而將卡片從終端裝置排出，並結束處理。

（8）終端裝置，當判斷卡片真僞認證資訊係爲正規者時，則對使用者要求提款金額等之更進一步的輸入操作。

（9）使用者依照要求，進行提款金額等的輸入操作。

（10）主電腦，係判斷提款金額等之輸入操作的內容是否爲適當。

（11）主電腦，當因爲存款量不足等之理由，而判斷提款金額等之輸入操作係爲不適當時，係將卡片從終端裝置排出，並結束處理。

（12）主電腦，當判斷提款金額等之輸入操作的內容係爲適當時，係進行提款等之輸出，並將卡片從終端裝置排出，而結束處理。

〔處理流程實施例 2〕

藉由圖 30，說明卡片真偽認證處理流程之實施例 2。

相對於在卡片真偽認證處理流程之實施例 1 中，係當卡片真偽認證資訊不正確時將卡片從終端裝置排出，此卡片真偽認證處理流程之實施例 2，當真偽認證資訊係爲不正確時，係將卡片取入至終端裝置中，並發出警報。藉由如此處理，成爲容易對不正當卡片作舉發。

（1）若是卡片之持有者將箭頭部作爲前端而將金融卡插入 ATM 等之終端裝置的卡片插入口內，則卡片插入口之感測器係感測有此，而將卡片取入至裝置內。

（2）當取入卡片時，終端裝置係從卡片之磁性記錄部而讀取卡片資訊。

（3）終端裝置，係判斷被插入之卡片是否爲此終端裝置所能處理的卡片。

（4）當從所讀取之卡片資訊中，無法確認有顯示此卡片係爲可處理的資訊的情況，又或是雖然係爲正當之卡片，卻因爲破損又或是污損等而造成無法讀取出卡片之資訊時，則終端裝置係將此卡片作爲無法處理之不適當卡片而排出之。

（5）終端裝置，係利用在取入卡片時之卡片的移動而作機械掃瞄，或是在卡片被取入並停止的狀態下，從真偽認證晶片讀取出真偽認證資訊。

（6）終端裝置，係判斷被讀取之卡片真偽認證資訊是否爲正確。

（7）當終端裝置判斷卡片真僞認證資訊係爲不正確時，係將被插入之卡片判斷爲非正規者，而將卡片取入至終端裝置中，並同時發出警報。。

此警報，若是成爲僅在遠離終端機之處發出，並在終端機係顯示爲故障，則成爲能容易地將不正規之卡片的使用者拘束。

（8）終端裝置，當判斷卡片真僞認證資訊係爲正規者時，則對使用者要求提款金額等之更進一步的輸入操作。

（9）使用者依照要求，進行提款金額等的輸入操作。

（10）主電腦，係判斷提款金額等之輸入操作的內容是否爲適當。

（11）主電腦，當因爲存款量不足等之理由，而判斷提款金額等之輸入操作係爲不適當時，係將卡片從終端裝置排出，並結束處理。

（12）主電腦，當判斷提款金額等之輸入操作的內容係爲適當時，係進行提款等之輸出，並將卡片從終端裝置排出，而結束處理。

〔處理流程實施例3〕

藉由圖31，說明卡片真僞認證處理流程之實施例3。

相對於在卡片真僞認證處理流程之實施例2中，係當卡片真僞認證資訊不正確時，直接將卡片取入終端裝置，

並發出警報，此卡片真偽認證處理流程之實施例 3，係使卡片利用者進行操作。

藉由如此處理，成爲能確實地對不正當卡片作舉發。

（1）若是卡片之持有者將箭頭部作爲前端而將金融卡插入 ATM 等之終端裝置的卡片插入口內，則卡片插入口之感測器係感測有此，而將卡片取入至裝置內。

（2）當取入卡片時，終端裝置係從卡片之磁性記錄部而讀取卡片資訊。

（3）終端裝置，係判斷被插入之卡片是否爲此終端裝置所能處理的卡片。

（4）當從所讀取之卡片資訊中，無法確認有顯示此卡片係爲可處理的資訊的情況，又或是雖然係爲正當之卡片，卻因爲破損又或是污損等而造成無法讀取出卡片之資訊時，則終端裝置係將此卡片作爲無法處理之不適當卡片而排出之。

（5）終端裝置，係利用在取入卡片時之卡片的移動而作機械掃瞄，或是在卡片被取入並停止的狀態下，從真偽認證晶片讀取出真偽認證資訊。

（6）終端裝置，係判斷被讀取之卡片真偽認證資訊是否爲正確。

（7）終端裝置，當判斷卡片真偽認證資訊係爲不正確時，則對使用者要求提款金額等之更進一步的輸入操作。

（8）使用者係依據要求，進行提款金額等的輸入操

作。

（9）在將卡片收容於終端裝置內的同時，發出警報。

此警報，若是成爲僅在遠離終端機之處發出，並在終端機係顯示爲故障，則成爲能容易地將不正規之卡片的使用者拘束。

（10）終端裝置，當判斷卡片真僞認證資訊係爲正規者時，則對使用者要求提款金額等之更進一步的輸入操作。

（11）使用者係依據要求，進行提款金額等的輸入操作。

（12）主電腦，係判斷提款金額等之輸入操作的內容是否爲適當。

（14）主電腦，當因爲存款量不足等之理由，而判斷提款金額等之輸入操作係爲不適當時，係將卡片從終端裝置排出，並結束處理。

藉由採用此種構成，不僅是使不正規卡片之使用者使用終端裝置的時間變長而使得將其拘束之時間變長，亦可藉由使其進行操作，而成爲可作指紋等之證據的採取。

此時，若是採用接觸型之觸控式面板，則係成爲能更確實地將指紋作採取。

〔產業上之利用可能性〕

以上所說明之真僞認證晶片、具備有卡片真僞認證晶

片之卡片，係可作爲銀行金融卡、信用卡、預付卡、點數卡、證券、ID卡、機構通行證、證明書等來採用。

【圖式簡單說明】

[圖 1]現行之金融卡處理流程圖

[圖 2]先前之金融卡的說明圖

[圖 3]使用人工物特徵辨識之先前的卡片之例

[圖 4]使用人工物特徵辨識之先前的卡片的其他例

[圖 5]被安裝有真僞認證晶片的卡片之例

[圖 6]被安裝有真僞認證晶片的卡片之其他例

[圖 7]被安裝有真僞認證晶片的卡片之另外其他例

[圖 8]真僞認證晶片的安裝位置之例的說明圖

[圖 9]真僞認證晶片的安裝位置之其他例的說明圖

[圖 10]位置對準用之記號的說明圖

[圖 11]根據亂數而作成之真僞認證晶片之例

[圖 12]使用於真僞認證晶片的亂數之例

[圖 13]使用於真僞認證晶片的亂數之配列例

[圖 14]將使用於真僞認證晶片的亂數設爲 2 進位數之例

[圖 15]將使用於真僞認證晶片的亂數作爲 2 進位數而配列之例

[圖 16]使用於真僞認證晶片的亂數之追加例

[圖 17]將使用於真僞認證晶片的追加亂數設爲 2 進位數之例

[圖 18]將使用於真僞認證晶片的追加亂數設爲 4 進位數之例

[圖 19]將使用於真僞認證晶片的亂數作爲 4 進位數而配列之例

[圖 20]從根據亂數而作成之真僞認證晶片，得到其他之真僞認證晶片之例

[圖 21]真僞認證晶片與被安裝有真僞認證晶片的卡片之例

[圖 22]圖 21 之卡片的真僞證明流程

[圖 23]真僞認證晶片與被安裝有真僞認證晶片的卡片之其他例

[圖 24]圖 23 之卡片的真僞證明流程

[圖 25]真僞認證晶片與被安裝有真僞認證晶片的卡片之另外其他例

[圖 26]圖 25 之卡片的真僞證明流程

[圖 27]真僞認證晶片與被安裝有真僞認證晶片的卡片之另外其他例

[圖 28]圖 27 之卡片的真僞證明流程

[圖 29]本申請之發明的金融卡處理流程圖

[圖 30]本申請之發明的其他金融卡處理流程圖

[圖 31]本申請之發明的另外其他金融卡處理流程圖

【主要元件符號說明】

1：卡片

98年11月25日修正替換頁

2：磁性條

3：箭頭

4、8、12、15、18、21、22、32、42、46、61：真偽認證晶片

5：金屬粒

6、14、34、44：表面板

7、35、45：卡片基板

9：網格構件

10：短小纖維

11、31、41：真偽認證卡片

16、19、22、23、25：凹坑

17、20、24：反射凹坑

33：螢光體粒子

43：放射性物質粒子

47：IC晶片

48：位置對準用記號

49：移動方向讀取開始線

50：移動方向讀取結束線

51、52：端部指示線

62、64、66、68：真偽證明晶片

60、63、65、67：真偽證明卡片

十、申請專利範圍

1. 一種真偽認證對象物，係爲有必要作真偽認證的對象物，其特徵爲：

於前述對象物中，係以不可將其從前述對象物所分離的方式，而被附加了被設置有將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案（artifact metrics pattern）資訊與讀取位置對位用記號之真偽認證晶片。

2. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，前述人工物特徵辨識圖案資訊，係爲由壓花全像圖所成。

3. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，前述人工物特徵辨識圖案資訊，係爲由放射性物質粒所成。

4. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，前述人工物特徵辨識圖案資訊，係爲由螢光物質粒所成。

5. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，係爲人爲之圖案資訊。

6. 如申請專利範圍第 5 項所記載之真偽認證對象物，其中，前述人爲之圖案資訊，係爲由壓花全像圖所成。

7. 如申請專利範圍第 5 項所記載之真偽認證對象物，其中，前述人爲之圖案資訊，係爲由放射性物質粒所成。

8. 如申請專利範圍第 5 項所記載之真偽認證對象物，其中，前述人爲之圖案資訊，係爲由螢光物質粒所成。

9. 如申請專利範圍第 5 項所記載之真偽認證對象物，其中，前述人爲之圖案資訊，係爲被配置爲矩陣狀之數位資料，而前述數位資料，係根據二進位亂數而被決定。

10. 如申請專利範圍第 9 項所記載之真偽認證對象物，其中，前述人爲之圖案資訊，係爲前述被配置爲矩陣狀之數位資料中之一部分。

11. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，前述讀取位置對位用記號，係爲 1 個。

12. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，前述讀取位置對位用記號，係爲複數個。

13. 如申請專利範圍第 1 項所記載之真偽認證對象物，其中，係被設置有讀取開始線、讀取結束線以及讀取端部指示線。

14. 如申請專利範圍第 11 項、第 12 項或第 13 項所記載之真偽認證對象物，其中，係更進而被設置有讀取同步訊號用之記號。

15. 一種真偽認證對象物，係爲有必要作真偽認證的

對象物，其特徵爲：

於前述對象物中，係以不可將其從前述對象物所分離的方式，而被附加有：被設置有將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊與讀取位置對位用記號之真僞認證晶片；和用以證明前述真僞認證晶片之真僞的資訊。

16. 如申請專利範圍第 15 項所記載之真僞認證對象物，其中，被設置有將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊與讀取位置對位用記號之真僞認證晶片，和用以證明前述真僞認證晶片之真僞的資訊，係被附加於不同之位置。

17. 如申請專利範圍第 15 項所記載之真僞認證對象物，其中，被設置有將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊與讀取位置對位用記號之真僞認證晶片，和用以證明前述真僞認證晶片之真僞的資訊，係被附加於相同之位置。

18. 如申請專利範圍第 15 項、第 16 項或第 17 項所記載之真僞認證對象物，其中，前述人工物特徵辨識圖案資訊，係爲由壓花全像圖所成。

19. 如申請專利範圍第 15 項、第 16 項或第 17 項所記載之真僞認證對象物，其中，前述人工物特徵辨識圖案資訊，係爲由放射性物質粒所成。

20. 如申請專利範圍第 15 項、第 16 項或第 17 項所記載之真僞認證對象物，其中，前述人工物特徵辨識圖案

資訊，係爲由螢光物質粒所成。

21. 如申請專利範圍第 15 項所記載之真僞認證對象物，其中，將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，係爲人爲之圖案資訊。

22. 如申請專利範圍第 21 項所記載之真僞認證對象物，其中，前述人爲之圖案資訊，係爲由壓花全像圖所成。

23. 如申請專利範圍第 21 項所記載之真僞認證對象物，其中，前述人爲之圖案資訊，係爲由放射性物質粒所成。

24. 如申請專利範圍第 21 項所記載之真僞認證對象物，其中，前述人爲之圖案資訊，係爲由螢光物質粒所成。

25. 如申請專利範圍第 21 項所記載之真僞認證對象物，其中，前述人爲之圖案資訊，係爲被配置爲矩陣狀之數位資料，而前述數位資料，係根據二進位亂數而被決定。

26. 如申請專利範圍第 21 項所記載之真僞認證對象物，其中，前述人爲之圖案資訊，係爲前述被配置爲矩陣狀之數位資料中之一部分。

27. 如申請專利範圍第 15 項所記載之真僞認證對象物，其中，前述讀取位置對位用記號，係爲 1 個。

28. 如申請專利範圍第 15 項所記載之真僞認證對象

物，其中，前述讀取位置對位用記號，係爲複數個。

29. 如申請專利範圍第 15 項所記載之真僞認證對象物，其中，係被設置有讀取開始線、讀取結束線以及讀取端部指示線。

30. 如申請專利範圍第 27 項、第 28 項或第 29 項所記載之真僞認證對象物，其中，係更進而被設置有讀取同步訊號用之記號。

31. 如申請專利範圍第 15 項所記載之真僞認證對象物，其中，用以證明前述真僞認證晶片之真僞的資訊，係爲根據對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，所得到之加密化的資料。

32. 如申請專利範圍第 31 項所記載之真僞認證對象物，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，作加密化後所得到之加密化資料。

33. 如申請專利範圍第 31 項所記載之真僞認證對象物，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊的雜湊（hash）值，作加密化後所得到之加密化資料。

34. 如申請專利範圍第 31 項所記載之真僞認證對象物，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，與由前述對象物之識別資訊所成之資訊，作加密化後所得到之加密化資料。

35. 如申請專利範圍第 31 項所記載之真偽認證對象物，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，與由電子浮水印所成之資訊，作加密化後所得到之加密化資料。

36. 如申請專利範圍第 31 項、第 32 項、第 33 項、第 34 項或第 35 項所記載之真偽認證對象物，其中，前述加密化資料，係爲使用由前述真偽認證對象物之發行者所管理之共通金鑰系統的共通金鑰而被加密化。

37. 如申請專利範圍第 31 項、第 32 項、第 33 項、第 34 項或第 35 項所記載之真偽認證對象物，其中，前述加密化資料，係爲使用由前述真偽認證對象物之發行者所管理之公開金鑰系統的公開金鑰而被加密化。

38. 如申請專利範圍第 31 項、第 32 項、第 33 項、第 34 項或第 35 項所記載之真偽認證對象物，其中，前述加密化資料，係爲使用由前述真偽認證對象物之發行者所管理之公開金鑰系統的秘密金鑰而被加密化。

39. 一種真偽認證系統，係爲進行對象物之真偽認證的系統，其特徵爲：

於前述對象物中，係以不可將其從前述對象物所分離的方式，而被附加有：

被設置有將前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊與讀取位置對位用記號之真偽認證晶片；和

用以證明前述對象物之真僞的真僞證明晶片，

而藉由將真僞認證晶片與前述真僞證明晶片作對照，來判定前述對象物的真僞。

40. 如申請專利範圍第 39 項所記載之真僞認證系統，其中，將前述對象物作特定之固有的不可複製之資訊，係爲人爲之圖案資訊。

41. 如申請專利範圍第 39 項所記載之真僞認證系統，其中，用以證明前述對象物之真僞的資訊，係爲根據對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，所得到之加密化的資料。

42. 如申請專利範圍第 41 項所記載之真僞認證系統，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊作加密化後，所得到之加密化資料。

43. 如申請專利範圍第 41 項所記載之真僞認證系統，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊的雜湊（hash）值作加密化後，所得到之加密化資料。

44. 如申請專利範圍第 41 項所記載之真僞認證系統，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，與由前述對象物之識別資訊所成之資訊，作加密化後所得到之加密化資料。

45. 如申請專利範圍第 41 項所記載之真僞認證系

統，其中，前述加密化資料，係爲將對前述對象物作特定之偶然所得到的固有的不可複製之人工物特徵辨識圖案資訊，與由電子浮水印所成之資訊，作加密化後所得到之加密化資料。

46. 如申請專利範圍第 41 項、第 42 項、第 43 項、第 44 項或第 45 項所記載之真僞認證系統，其中，前述加密化資料，係爲使用由前述真僞認證對象物之發行者所管理之共通金鑰系統的共通金鑰而被加密化。

47. 如申請專利範圍第 41 項、第 42 項、第 43 項、第 44 項或第 45 項所記載之真僞認證系統，其中，前述加密化資料，係爲使用由前述真僞認證對象物之發行者所管理之公開金鑰系統的公開金鑰而被加密化。

48. 如申請專利範圍第 41 項、第 42 項、第 43 項、第 44 項或第 45 項所記載之真僞認證系統，其中，前述加密化資料，係爲使用由前述真僞認證對象物之發行者所管理之公開金鑰系統的祕密金鑰而被加密化。

圖1

764192

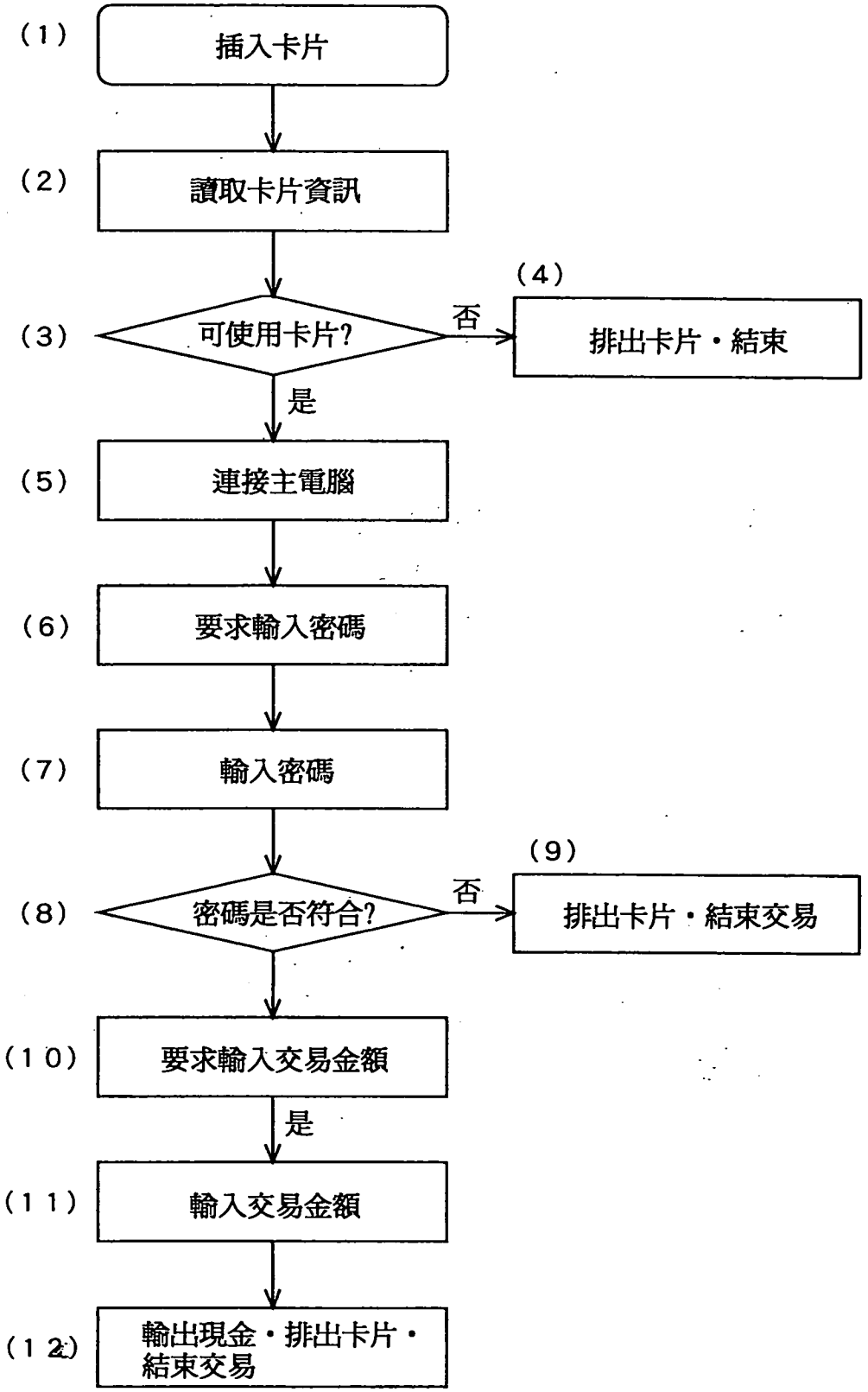
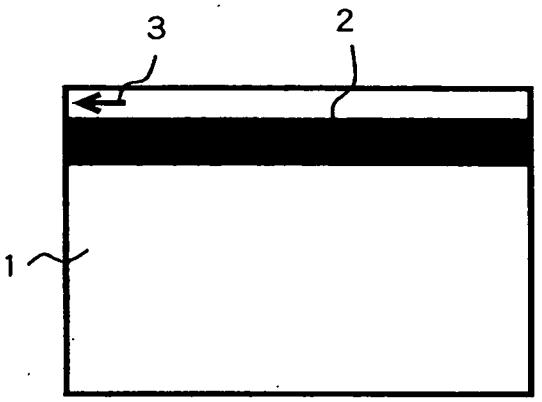
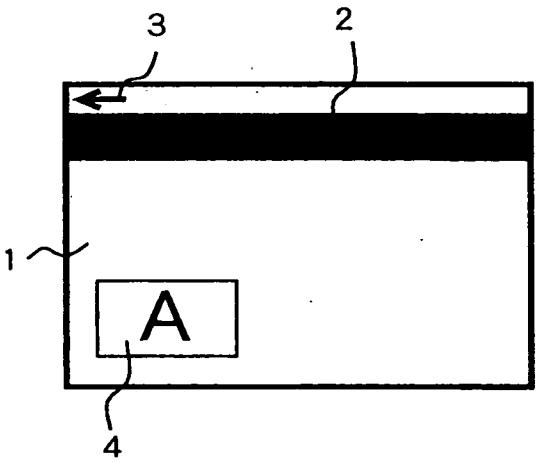

(1)
插入卡片
(2)
讀取卡片資訊
(3)
可使用卡片?
否
(4)
排出卡片・結束
是
(5)
連接主電腦
(6)
要求輸入密碼
(7)
輸入密碼
(8)
密碼是否符合?
否
(9)
排出卡片・結束交易
(10)
要求輸入交易金額
是
(11)
輸入交易金額
(12)
輸出現金・排出卡片・結束交易

圖2



(a)



(b)

圖3

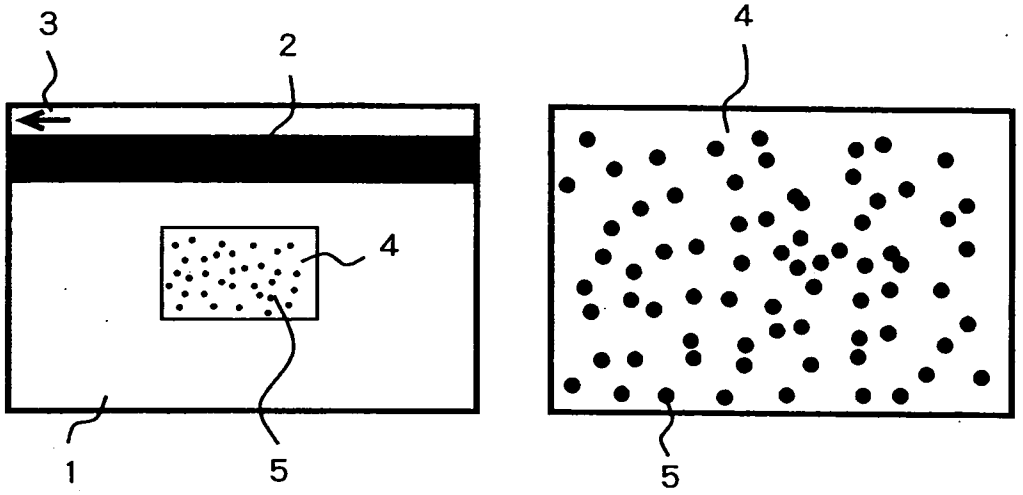
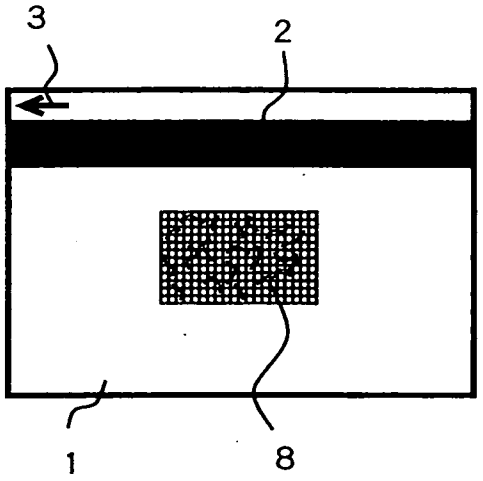
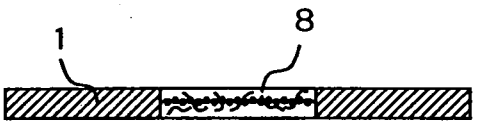


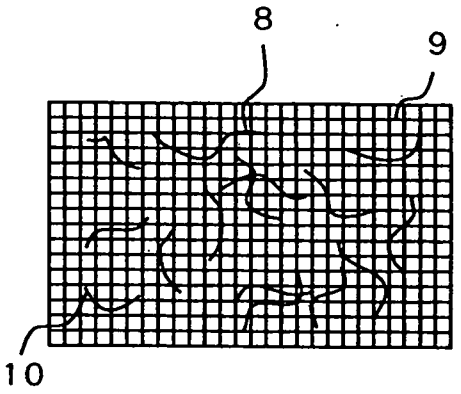
圖4



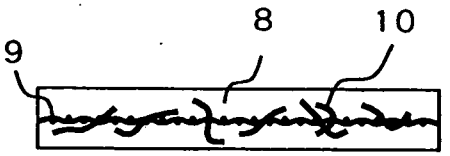
(a)



(b)



(c)



(d)

圖5

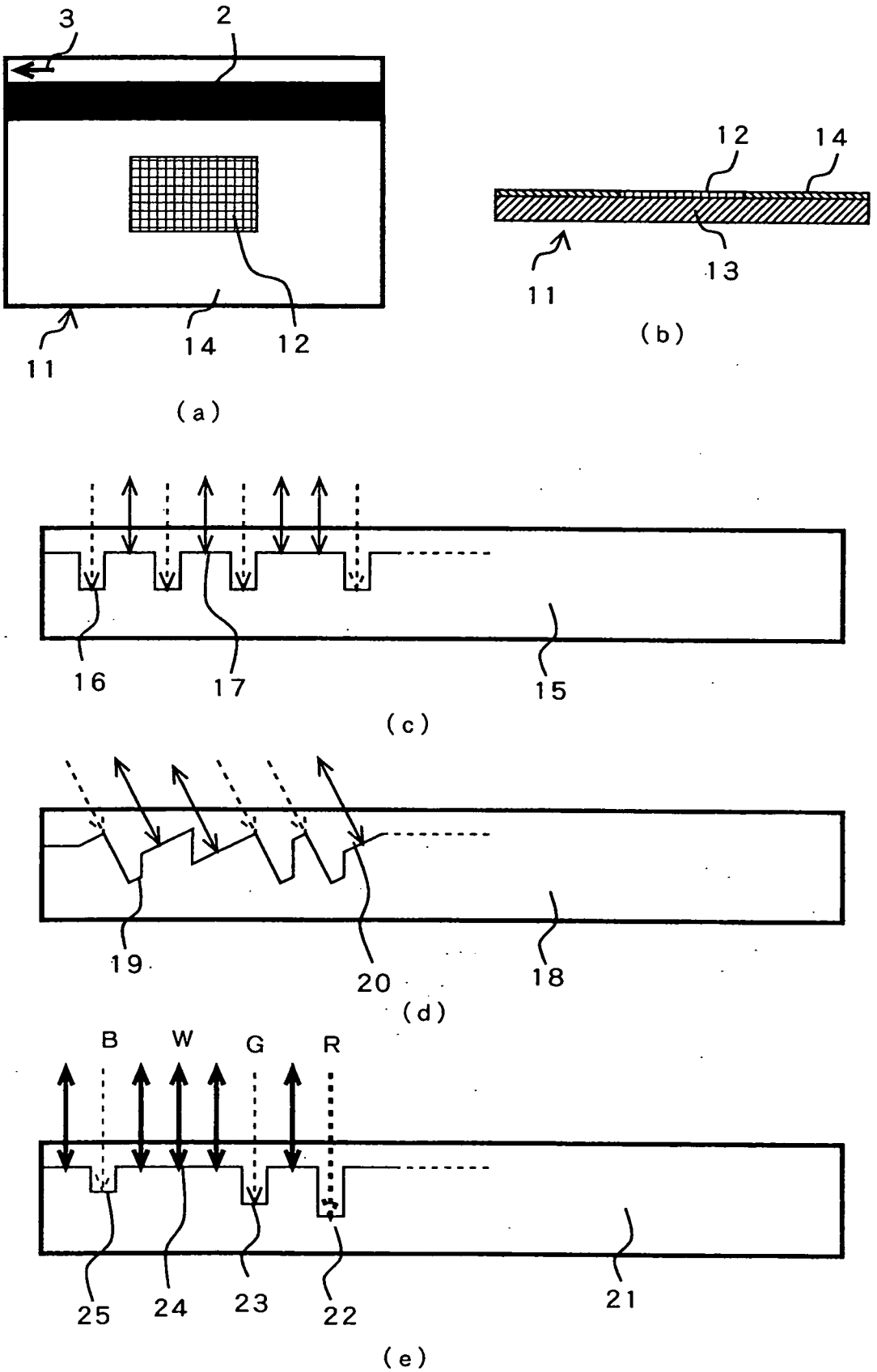


圖6

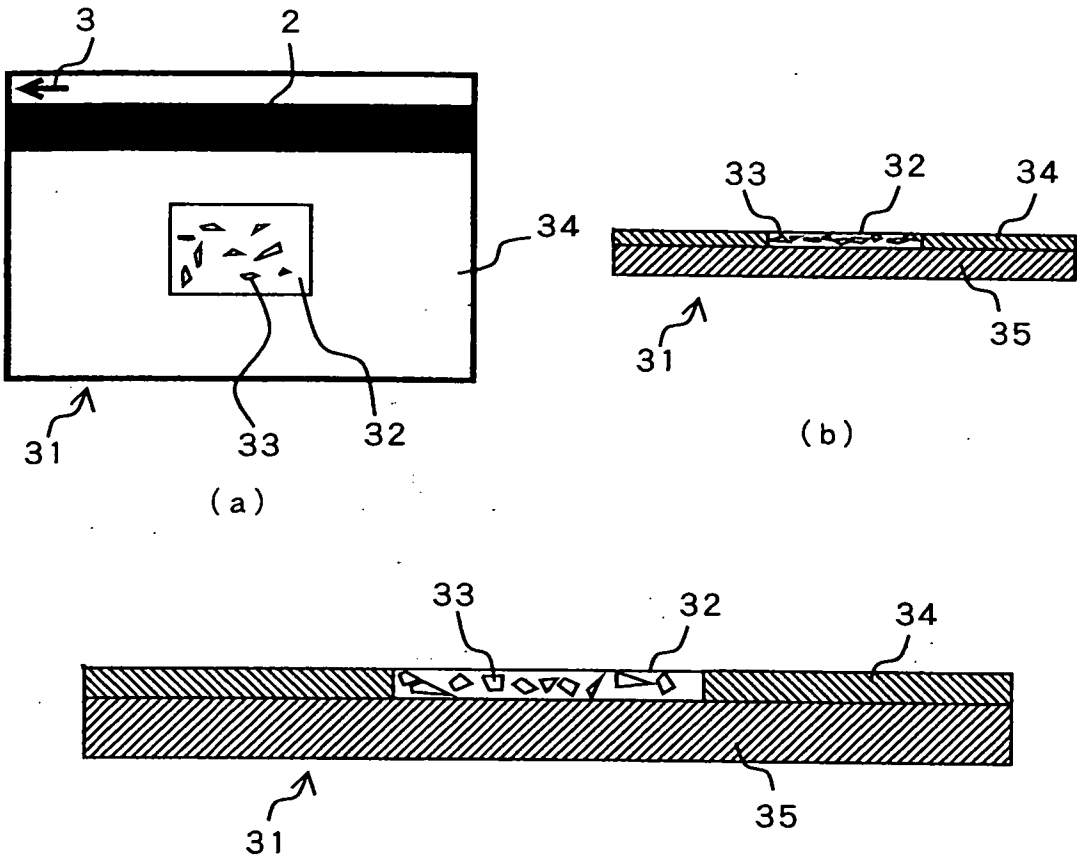


圖7

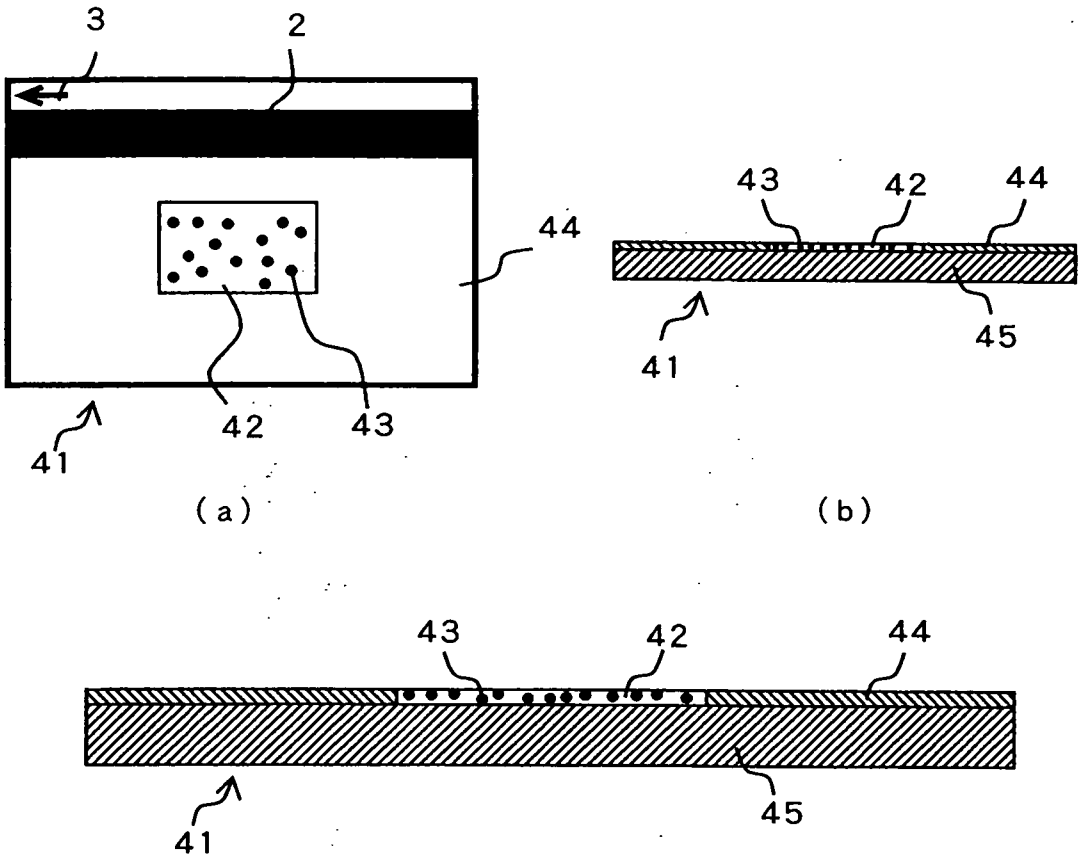


圖8

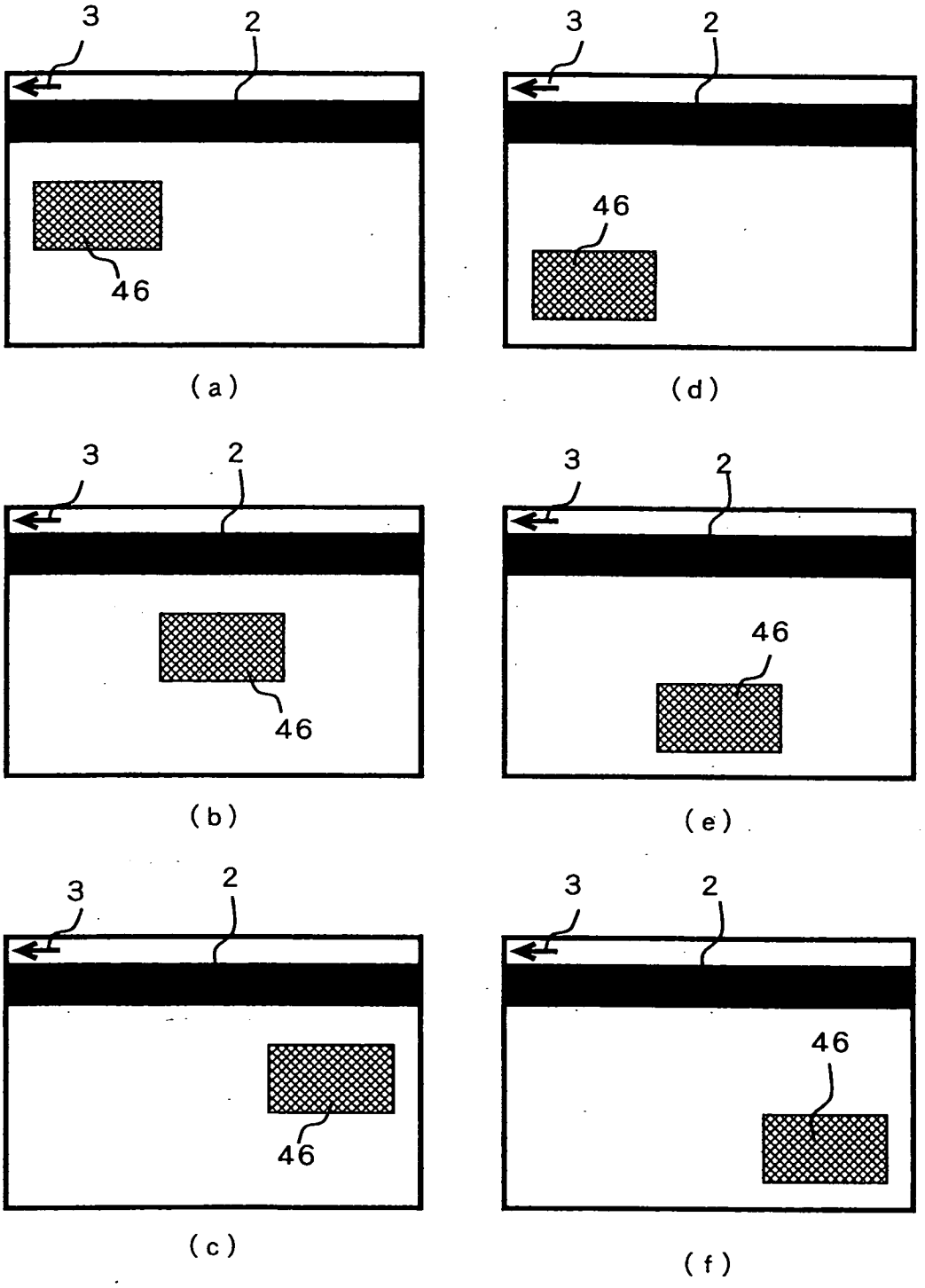


圖9

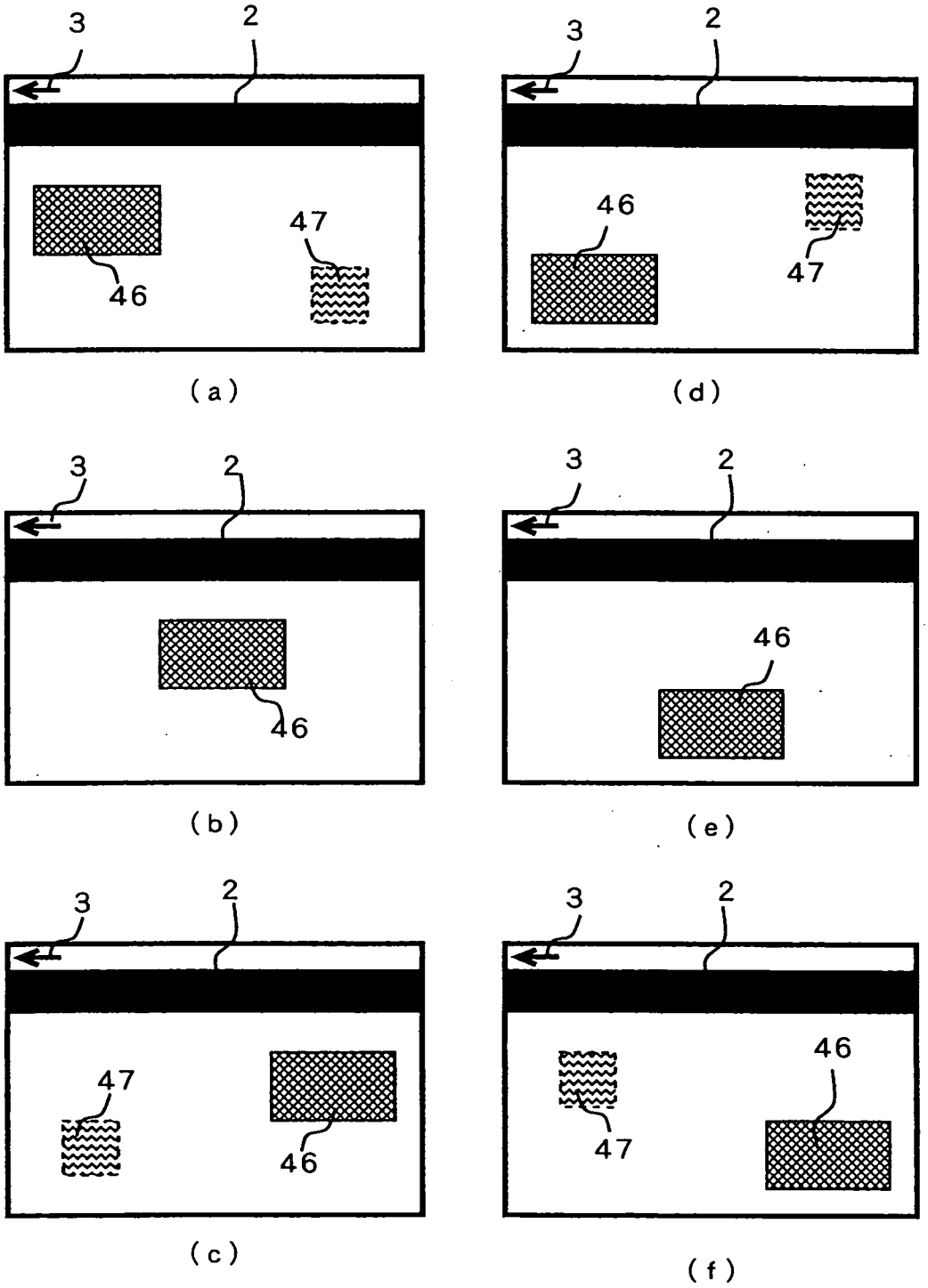


圖10

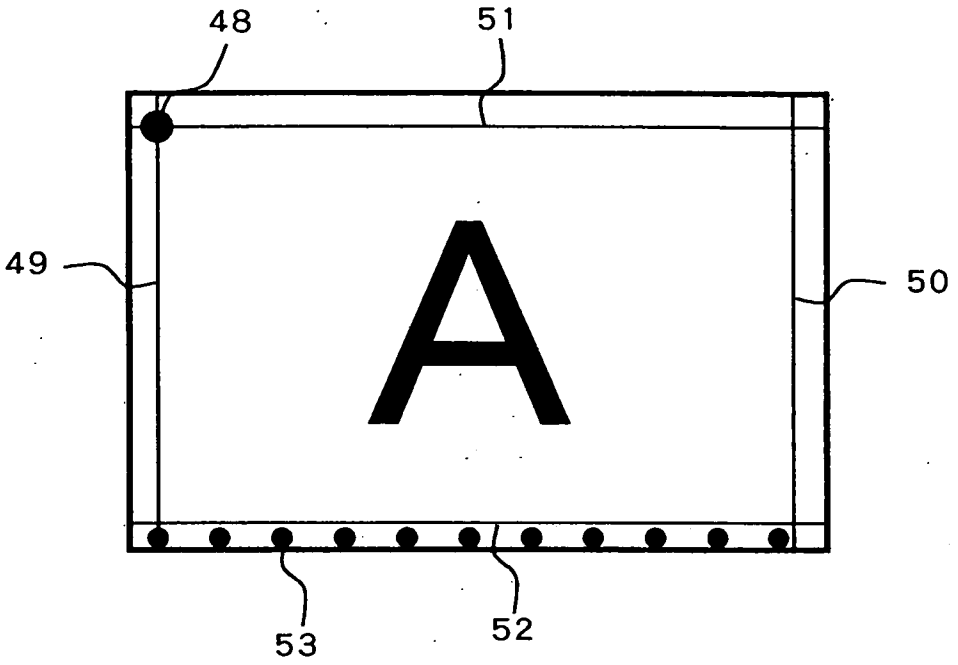


圖11

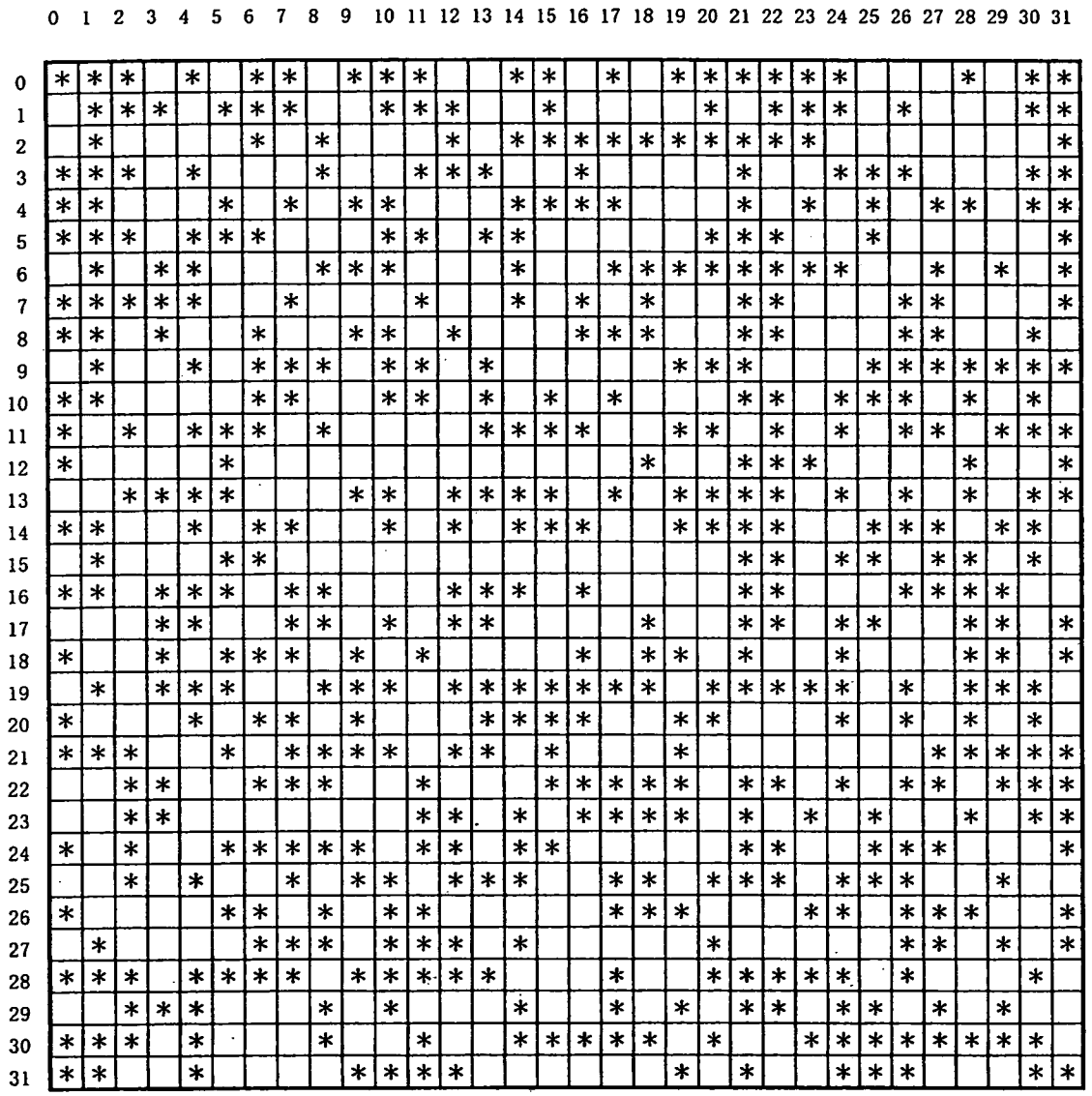

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0 *
1 *
2 *
3 *
4 *
5 *
6 *
7 *
8 *
9 *
10 *
11 *
12 *
13 *
14 *
15 *
16 *
17 *
18 *
19 *
20 *
21 *
22 *
23 *
24 *
25 *
26 *
27 *
28 *
29 *
30 *
31 *

圖12

EB735F8B77390BA3428BFF01E89C84E3
C563C55BEE360E4158E27F95F912A631
D268E6324BB41C7FC33546EAAE879AB7
840027093C6F5EABCB2B9E76460006DA
DD8E863C19AC26CD9750B48D5CEFEFAE
8B4798AAE5ED101F3391F6B7301AF54B
A7DB0671296E6EE486B071B943BA0835
EF7C4FA238A256D4E893E9FEC87814E3

圖13

E	B	7	3	5	F	8	B
7	7	3	9	0	B	A	3
4	2	8	B	F	F	0	1
E	B	7	3	5	F	8	B
7	7	3	9	0	B	A	3
4	2	8	B	F	F	0	1
E	8	9	C	8	4	E	3
C	5	6	3	C	5	5	B
E	E	3	6	0	E	4	1
5	8	E	2	7	F	9	5
F	9	1	2	A	6	3	1
D	2	6	8	E	6	3	2
4	B	B	4	1	C	7	F
C	3	3	5	4	6	E	A
A	E	8	7	9	A	B	7
8	4	0	0	2	7	0	9
3	C	6	F	5	E	A	B
C	B	2	B	9	E	7	6
4	6	0	0	0	6	D	A
D	D	8	E	8	6	3	C
1	9	A	C	2	6	C	D
9	7	5	0	B	4	8	D
5	C	E	F	E	F	A	E
8	B	4	7	9	8	A	A
E	5	E	D	1	0	1	F
3	3	9	1	F	6	B	7
3	0	1	A	F	5	4	B
A	7	D	B	0	6	7	1
2	9	6	E	6	E	E	4
8	6	B	0	7	1	B	9
4	3	B	A	0	8	3	5
E	F	7	C	4	F	A	2
3	8	A	2	5	6	D	4
E	8	9	3	E	9	F	E
C	8	7	8	1	4	E	3

圖14

1110, 1011, 0111, 0011, 0101, 1111, 1000, 1011,
0111, 0111, 0011, 1001, 0000, 1011, 1010, 0011,
0100, 0010, 1000, 1011, 1111, 1111, 0000, 0001,
1110, 1000, 1001, 1100, 1000, 0100, 1110, 0011,
1100, 0101, 0110, 0011, 1100, 0101, 0101, 1011,
1110, 1110, 0011, 0110, 0000, 1110, 0100, 0001,
0101, 1000, 1110, 0010, 0111, 1111, 1001, 0101,
1111, 1001, 0001, 0010, 1010, 0110, 0011, 0001,
1101, 0010, 0110, 1000, 1110, 0110, 0011, 0010,
0100, 1011, 1011, 0100, 0001, 1100, 0111, 1111,
1100, 0011, 0011, 0101, 0100, 0110, 1110, 1010,
1010, 1110, 1000, 0111, 1001, 1010, 1011, 0111,
1000, 0100, 0000, 0000, 0010, 0111, 0000, 1001,
0011, 1100, 0110, 1111, 0101, 1110, 1010, 1011,
1100, 1011, 0010, 1011, 1001, 1110, 0111, 0110,
0100, 0110, 0000, 0000, 0000, 0110, 1101, 1010,
1101, 1101, 1000, 1110, 1000, 0110, 0011, 1100,
0001, 1001, 1010, 1100, 0010, 0110, 1100, 1101,
1001, 0111, 0101, 0000, 1011, 0100, 1000, 1101,
0101, 1100, 1110, 1111, 1110, 1111, 1010, 1110,
1000, 1011, 0100, 0111, 1001, 1000, 1010, 1010,
1110, 0101, 1110, 1101, 0001, 0000, 0001, 1111,
0011, 0011, 1001, 0001, 1111, 0110, 1011, 0111,
0011, 0000, 0001, 1010, 1111, 0101, 0100, 1011,
1010, 0111, 1101, 1011, 0000, 0110, 0111, 0001,
0010, 1001, 0110, 1110, 0110, 1110, 1110, 0100,
1000, 0110, 1011, 0000, 0111, 0001, 1011, 1001,
0100, 0011, 1011, 1010, 0000, 1000, 0011, 0101,
1110, 1111, 0111, 1100, 0100, 1111, 1010, 0010,
0011, 1000, 1010, 0010, 0101, 0110, 1101, 0100,
1110, 1000, 1001, 0011, 1110, 1001, 1111, 1110,
1100, 1000, 0111, 1000, 0001, 0100, 1110, 0011,

圖15

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	1	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	0	1	0	1	1	1	1	1	1	0	0	0	1	0	1	1
1	0	1	1	1	0	1	1	1	0	0	1	1	1	0	0	1	0	0	0	0	1	0	1	1	1	0	1	0	0	0	1	1
2	0	1	0	0	0	0	1	0	1	0	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1
3	1	1	1	0	1	0	0	0	1	0	0	1	1	1	0	0	1	0	0	0	0	1	0	0	1	1	1	0	0	0	1	1
4	1	1	0	0	0	1	0	1	0	1	1	0	0	0	1	1	1	1	0	0	0	1	0	1	0	1	0	1	1	0	1	1
5	1	1	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	0	0	1	1	1	0	0	1	0	0	0	0	0	1
6	0	1	0	1	1	0	0	0	1	1	1	0	0	0	1	0	0	1	1	1	1	1	1	1	1	0	0	1	0	1	0	1
7	1	1	1	1	1	0	0	1	0	0	0	1	0	0	1	0	1	0	1	0	0	1	1	0	0	0	1	1	0	0	0	1
8	1	1	0	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	0	0	1	1	0	0	1	0
9	0	1	0	0	1	0	1	1	1	0	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	1	1	1	1	1	1	1
10	1	1	0	0	0	0	1	1	0	0	1	1	0	1	0	1	0	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0
11	1	0	1	0	1	1	1	0	1	0	0	0	0	1	1	1	1	0	0	1	1	0	1	0	1	0	1	1	0	1	1	1
12	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	1	0	0	1
13	0	0	1	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1	0	1	1	1	1	0	1	0	1	0	1	0	1	1
14	1	1	0	0	1	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	1	1	0	0	1	1	1	0	1	1	0
15	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0
16	1	1	0	1	1	1	0	1	1	0	0	0	1	1	1	0	1	0	0	0	0	1	1	0	0	0	1	1	1	1	0	0
17	0	0	0	1	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	1
18	1	0	0	1	0	1	1	1	0	1	0	1	0	0	0	0	1	0	1	1	0	1	0	0	1	0	0	0	1	1	0	1
19	0	1	0	1	1	1	0	0	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	0	1	1	1	0
20	1	0	0	0	1	0	1	1	0	1	0	0	0	1	1	1	1	0	0	1	1	0	0	0	1	0	1	0	1	0	1	0
21	1	1	1	0	0	1	0	1	1	1	1	0	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1
22	0	0	1	1	0	0	1	1	1	0	0	1	0	0	0	1	1	1	1	1	0	1	1	0	1	0	1	1	0	1	1	1
23	0	0	1	1	0	0	0	0	0	0	0	1	1	0	1	0	1	1	1	1	0	1	0	1	0	1	0	0	1	0	1	1
24	1	0	1	0	0	1	1	1	1	1	0	1	1	0	1	1	0	0	0	0	0	1	1	0	0	1	1	1	0	0	0	1
25	0	0	1	0	1	0	0	1	0	1	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	1	1	0	0	1	0	0
26	1	0	0	0	0	1	1	0	1	0	1	1	0	0	0	0	0	1	1	1	0	0	0	1	1	0	1	1	1	0	0	1
27	0	1	0	0	0	0	1	1	1	0	1	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	1	0	1	0	1
28	1	1	1	0	1	1	1	1	0	1	1	1	1	1	0	0	0	1	0	0	1	1	1	1	1	0	1	0	0	0	1	0
29	0	0	1	1	1	0	0	0	1	0	1	0	0	0	1	0	0	1	0	1	0	1	1	0	1	1	0	1	0	1	0	0
30	1	1	1	0	1	0	0	0	1	0	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	0
31	1	1	0	0	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	1	1

圖16

16進亂數列 b

7EDD7E7E7CD7DFD91AA59CD33ED11718
A982D1571419199DE37A9BC2C4D88D02
CB206356D9A624F85403C8525A822CB0
2590C020CBF7BBDF02112B9966B7CBF8
DCADB34B1D912D304FEE9F3D7FF8D7EC
5B5A505293EC1732E0B1845AE55B5720
55BCEA8129C1E5D043AE3A31076C8E1A
9EB0063128535 3D708F9C2C0FFEDCF7E

16進亂數列 a

EB735F8B773 90BA3428BFF01E89C84E3
C563C55BEE360E4158E27F95F912A631
D268E6324BB41C7FC33546EAAE879AB7
8400270 93C6F5EABCB2B9E7646 0006DA
DD8E863C19AC26CD9750B48D5CEFEFAE
8B4798AAE5ED101F3391F6B7301AF54B
A7DB0671296E6EE486B071B943BA0835
EF7C4FA238A256D4E893E9FEC87814E3

圖17

2進亂數列 b

01, 11, 11, 10, 11, 01, 11, 01, 01, 11, 11, 10, 01, 11, 11, 10,
01, 11, 11, 00, 11, 01, 01, 11, 11, 01, 11, 11, 11, 01, 10, 01,
00, 01, 10, 10, 10, 10, 01, 01, 10, 01, 11, 00, 11, 01, 00, 11,
00, 11, 11, 10, 11, 01, 00, 01, 00, 01, 01, 11, 00, 01, 10, 00,
10, 10, 10, 01, 10, 00, 00, 10, 11, 01, 00, 01, 01, 01, 01, 11,
00, 01, 01, 00, 00, 01, 10, 01, 00, 01, 10, 01, 10, 01, 11, 01,
11, 10, 00, 11, 01, 11, 10, 10, 10, 01, 10, 11, 11, 00, 00, 10,
11, 00, 01, 00, 11, 01, 10, 00, 10, 00, 11, 01, 00, 00, 00, 10,
11, 00, 10, 11, 00, 10, 00, 00, 01, 10, 00, 11, 01, 01, 01, 10,
11, 01, 10, 01, 10, 10, 01, 10, 00, 10, 01, 00, 11, 11, 10, 00,
01, 01, 01, 00, 00, 00, 00, 11, 11, 00, 10, 00, 01, 01, 00, 10,
01, 01, 10, 10, 10, 00, 00, 10, 00, 10, 11, 00, 10, 11, 00, 00,
00, 10, 01, 01, 10, 01, 00, 00, 11, 00, 00, 00, 00, 10, 00, 00,
11, 00, 10, 11, 11, 11, 01, 11, 10, 11, 10, 11, 11, 01, 11, 11,
00, 00, 00, 10, 00, 01, 00, 01, 00, 10, 10, 11, 10, 01, 10, 01,
01, 10, 01, 10, 10, 11, 01, 11, 11, 00, 10, 11, 11, 11, 10, 00,
11, 01, 11, 00, 10, 10, 11, 01, 10, 11, 00, 11, 01, 00, 10, 11,
00, 01, 11, 01, 10, 01, 00, 01, 00, 10, 11, 01, 00, 11, 00, 00,
01, 00, 11, 11, 11, 10, 11, 10, 10, 01, 11, 11, 00, 11, 11, 01,
01, 11, 11, 11, 11, 11, 10, 00, 11, 01, 01, 11, 11, 10, 11, 00,
01, 01, 10, 11, 01, 01, 10, 10, 01, 01, 00, 00, 01, 01, 00, 10,
10, 01, 00, 11, 11, 10, 11, 00, 00, 01, 01, 11, 00, 11, 00, 10,
11, 10, 00, 00, 10, 11, 00, 01, 10, 00, 01, 00, 01, 01, 10, 10,
11, 10, 01, 01, 01, 01, 10, 11, 01, 01, 01, 11, 00, 10, 00, 00,
01, 01, 01, 01, 10, 11, 11, 00, 11, 10, 10, 10, 10, 00, 00, 01,
00, 10, 10, 01, 11, 00, 00, 01, 11, 10, 01, 01, 11, 01, 00, 00,
01, 00, 00, 11, 10, 10, 11, 10, 00, 11, 10, 10, 00, 11, 00, 01,
00, 00, 01, 11, 01, 10, 11, 00, 10, 00, 11, 10, 00, 01, 10, 10,
10, 01, 11, 10, 10, 11, 00, 00, 00, 00, 01, 10, 00, 11, 00, 01,
00, 10, 10, 00, 01, 01, 00, 11, 01, 01, 00, 11, 11, 01, 01, 11,
00, 00, 10, 00, 11, 11, 10, 01, 11, 00, 00, 10, 11, 00, 00, 00,
11, 11, 11, 11, 11, 11, 10, 11, 01, 11, 00, 11, 11, 01, 11, 11, 10,

2進亂數列 a

11, 10, 10, 11, 01, 11, 00, 11, 01, 01, 11, 11, 10, 00, 10, 11,
01, 11, 01, 11, 00, 11, 10, 01, 00, 00, 10, 11, 10, 10, 00, 11,
01, 00, 00, 10, 10, 00, 10, 11, 11, 11, 11, 11, 00, 00, 00, 01,
11, 10, 10, 00, 10, 01, 11, 00, 10, 00, 01, 00, 11, 10, 00, 11,
11, 00, 01, 01, 01, 10, 00, 11, 11, 00, 01, 01, 01, 01, 10, 11,
11, 10, 11, 10, 00, 11, 01, 10, 00, 00, 11, 10, 01, 00, 00, 01,
01, 01, 10, 00, 11, 10, 00, 10, 01, 11, 11, 11, 10, 01, 01, 01,
11, 11, 10, 01, 00, 01, 00, 10, 10, 10, 01, 10, 00, 11, 00, 01,
11, 01, 00, 10, 01, 10, 10, 00, 11, 10, 01, 10, 00, 11, 00, 10,
01, 00, 10, 11, 10, 11, 01, 00, 00, 01, 11, 00, 01, 11, 11, 11,
11, 00, 00, 11, 00, 11, 01, 01, 01, 00, 01, 10, 11, 10, 10, 10,
10, 10, 11, 10, 10, 00, 01, 11, 10, 01, 10, 10, 10, 11, 01, 11,
10, 00, 01, 00, 00, 00, 00, 00, 10, 01, 11, 00, 00, 10, 01,
00, 11, 11, 00, 01, 10, 11, 11, 01, 01, 11, 10, 10, 10, 10, 11,
11, 00, 10, 11, 00, 10, 10, 11, 10, 01, 11, 10, 01, 11, 01, 10,
01, 00, 01, 10, 00, 00, 00, 00, 00, 00, 01, 10, 11, 01, 10, 10,
11, 01, 11, 01, 10, 00, 11, 10, 10, 00, 01, 10, 00, 11, 11, 00,
00, 01, 10, 01, 10, 10, 11, 00, 00, 10, 01, 10, 11, 00, 11, 01,
10, 01, 01, 11, 01, 01, 00, 00, 10, 11, 01, 00, 10, 00, 11, 01,
01, 01, 11, 00, 11, 10, 11, 11, 11, 10, 11, 11, 10, 10, 11, 10,
10, 00, 10, 11, 01, 00, 01, 11, 10, 01, 10, 00, 10, 10, 10, 10,
11, 10, 01, 01, 11, 10, 11, 01, 00, 01, 00, 00, 00, 01, 11, 11,
00, 11, 00, 11, 10, 01, 00, 01, 11, 11, 01, 10, 10, 11, 01, 11,
00, 11, 00, 00, 00, 01, 10, 10, 11, 11, 01, 01, 01, 00, 10, 11,
10, 10, 01, 11, 11, 01, 10, 11, 00, 00, 01, 10, 01, 11, 00, 01,
00, 10, 10, 01, 01, 10, 11, 10, 01, 10, 11, 10, 11, 10, 01, 00,
10, 00, 01, 10, 10, 11, 00, 00, 01, 11, 00, 01, 10, 11, 10, 01,
01, 00, 00, 11, 10, 11, 10, 10, 00, 00, 10, 00, 00, 11, 01, 01,
11, 10, 11, 11, 01, 11, 11, 00, 01, 00, 11, 11, 10, 10, 00, 10,
00, 11, 10, 00, 10, 10, 00, 10, 01, 01, 01, 10, 11, 01, 01, 00,
11, 10, 10, 00, 10, 01, 00, 11, 11, 10, 10, 01, 11, 11, 11, 10,
11, 00, 10, 00, 01, 11, 10, 00, 00, 01, 01, 00, 11, 10, 00, 11,

圖18

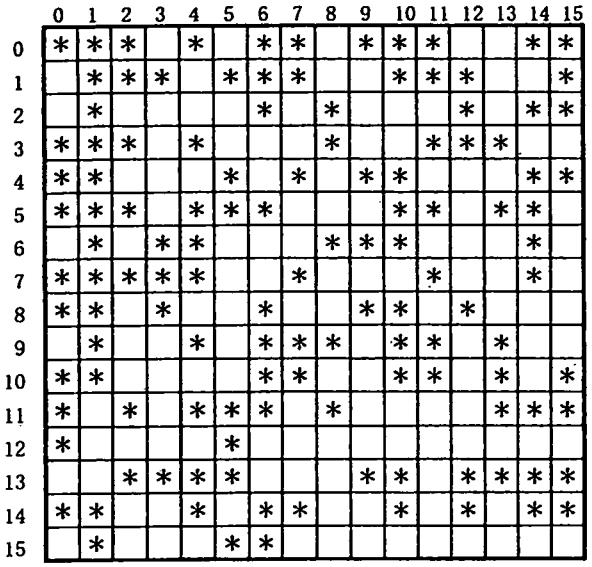
4進亂數列 b

R, B, B, G, B, R, B, R, R, B, B, G, R, B, B, G,
R, B, B, 0, B, R, R, B, B, R, B, B, B, R, G, R,
0, R, G, G, G, G, R, R, G, R, B, 0, B, R, 0, B,
0, B, B, G, B, R, 0, R, 0, R, R, B, 0, R, G, 0,
G, G, G, R, G, 0, 0, G, B, R, 0, R, G, R, R, B,
0, R, R, 0, 0, R, G, R, 0, R, G, R, G, R, B, R,
B, G, 0, B, R, B, G, G, G, R, G, B, B, 0, 0, G,
B, 0, R, 0, B, R, G, 0, G, 0, B, R, 0, 0, 0, G,
B, 0, G, B, 0, G, 0, 0, R, G, 0, B, R, R, R, G,
B, R, G, R, G, G, R, G, 0, G, R, 0, B, B, G, 0,
R, R, R, 0, 0, 0, 0, B, B, 0, G, 0, R, R, 0, G,
R, R, G, G, G, 0, 0, G, 0, G, B, 0, G, B, 0, 0,
0, G, R, R, G, R, 0, 0, B, 0, 0, 0, 0, G, 0, 0,
B, 0, G, B, B, B, R, B, G, B, G, B, B, R, B, B,
0, 0, 0, G, 0, R, 0, R, 0, G, G, B, G, R, G, R,
R, G, R, G, G, B, R, B, B, 0, G, B, B, B, G, 0,
B, R, B, 0, G, G, B, R, G, B, 0, B, R, 0, G, B,
0, R, B, R, G, R, 0, R, 0, G, B, R, 0, B, 0, 0,
R, 0, B, B, B, G, B, G, G, R, B, B, 0, B, B, R,
R, B, B, B, B, B, G, 0, B, R, R, B, B, G, B, 0,
R, R, G, B, R, R, G, G, R, R, 0, 0, R, R, 0, G,
G, R, 0, B, B, G, B, 0, 0, R, R, B, 0, B, 0, G,
B, G, 0, 0, G, B, 0, R, G, 0, R, 0, R, R, G, G,
B, G, R, R, R, R, G, B, R, R, R, B, 0, G, 0, 0,
R, R, R, R, G, B, B, 0, B, G, G, G, 0, 0, 0, R,
0, G, G, R, B, 0, 0, R, B, G, R, R, B, R, 0, 0,
R, 0, 0, B, G, G, B, G, 0, B, G, G, 0, B, 0, R,
0, 0, R, B, R, G, B, 0, G, 0, B, G, 0, R, G, G,
G, R, B, G, G, B, 0, 0, 0, 0, R, G, 0, B, 0, R,
0, G, G, 0, R, R, 0, B, R, R, 0, B, B, R, R, B,
0, 0, G, 0, B, B, G, R, B, 0, 0, G, B, 0, 0, 0,
B, B, B, B, B, G, B, R, B, 0, B, B, R, B, B, G,
4進亂數列 a
B, G, G, B, R, B, 0, B, R, R, B, B, G, 0, G, B,
R, B, R, B, 0, B, G, R, 0, 0, G, B, G, G, 0, B,
R, 0, 0, G, G, 0, G, B, B, B, B, 0, 0, 0, R,
B, G, G, 0, G, R, B, 0, G, 0, R, 0, B, G, 0, B,
B, 0, R, R, R, G, 0, B, B, 0, R, R, R, R, G, B,
B, G, B, G, 0, B, R, G, 0, 0, B, G, R, 0, 0, R,
R, R, G, 0, B, G, 0, G, R, B, B, B, G, R, R, R,
B, B, G, R, 0, R, 0, G, G, G, R, G, 0, B, 0, R,
B, R, 0, G, R, G, G, 0, B, G, R, G, 0, B, 0, G,
R, 0, G, B, G, B, R, 0, 0, R, B, 0, R, B, B, B,
B, 0, 0, B, 0, B, R, R, R, 0, R, G, B, G, G, G,
G, G, B, G, G, 0, R, B, G, R, G, G, G, B, R, B,
G, 0, R, 0, 0, 0, 0, 0, 0, G, R, B, 0, 0, G, R,
0, B, B, 0, R, G, B, B, R, R, B, G, G, G, G, B,
B, 0, G, B, 0, G, G, B, G, R, B, G, R, B, R, G,
R, 0, R, G, 0, 0, 0, 0, 0, 0, R, G, B, R, G, G,
B, R, B, R, G, 0, B, G, G, 0, R, G, 0, B, B, 0,
0, R, G, R, G, G, B, 0, 0, G, R, G, B, 0, B, R,
G, R, R, B, R, R, 0, 0, G, B, R, 0, G, 0, B, R,
R, R, B, 0, B, G, B, B, B, G, B, B, G, G, B, G,
G, 0, G, B, R, 0, R, B, G, R, G, 0, G, G, G, G,
B, G, R, R, B, G, B, R, 0, R, 0, 0, 0, R, B, B,
0, B, 0, B, G, R, 0, R, B, B, R, G, G, B, R, B,
0, B, 0, 0, 0, R, G, G, B, B, R, R, R, 0, G, B,
G, G, R, B, B, R, G, B, 0, 0, R, G, R, B, 0, R,
0, G, G, R, R, G, B, G, R, G, B, G, B, G, R, 0,
G, 0, R, G, G, B, 0, 0, R, B, 0, R, G, B, G, R,
R, 0, 0, B, G, B, G, G, 0, 0, G, 0, 0, B, R, R,
B, G, B, B, R, B, B, 0, R, 0, B, B, G, G, 0, G,
0, B, G, 0, G, G, 0, G, R, R, R, G, B, R, R, 0,
B, G, G, 0, G, R, 0, B, B, G, G, R, B, B, B, G,
B, 0, G, 0, R, B, G, 0, 0, R, R, 0, B, G, 0, B,

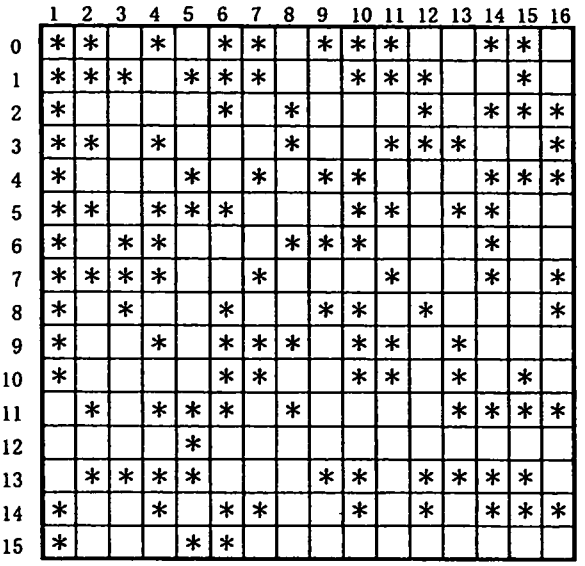
圖19

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	R	B	B	G	B	R	B	R	R	B	B	G	R	B	B	G	R	B	B	0	B	R	R	B	B	R	B	B	B	R	G	R
1	0	R	G	G	G	G	R	R	G	R	B	0	B	R	0	B	0	B	B	G	B	R	0	R	0	R	R	B	0	R	G	0
2	G	G	G	R	G	0	0	G	B	R	0	R	R	R	R	B	0	R	R	0	0	R	G	R	0	R	G	R	G	R	B	R
3	B	G	0	B	R	B	G	G	G	R	G	B	B	0	0	G	B	0	R	0	B	R	G	0	G	0	B	R	0	0	0	G
4	B	0	G	B	0	G	0	0	R	G	0	B	R	R	R	G	B	R	G	R	G	G	R	G	0	G	R	0	B	B	G	0
5	R	R	R	0	0	0	0	B	B	0	G	0	R	R	0	G	R	R	G	G	G	0	0	G	0	G	B	0	G	B	0	0
6	0	G	R	R	G	R	0	0	B	0	0	0	0	G	0	0	B	0	G	B	B	B	R	B	G	B	G	B	B	R	B	B
7	0	0	0	G	0	R	0	R	0	G	G	B	G	R	G	R	R	G	R	G	G	B	R	B	B	0	G	B	B	B	G	0
8	B	R	B	0	G	G	B	R	G	B	0	B	R	0	G	B	0	R	B	R	G	R	0	R	0	G	B	R	0	B	0	0
9	R	0	B	B	B	G	B	G	G	R	B	B	0	B	B	R	R	B	B	B	B	B	B	G	0	B	R	R	B	B	G	B	0
10	R	R	G	B	R	R	G	G	R	R	0	0	R	R	0	G	G	R	0	B	B	G	B	0	0	R	R	B	0	B	0	G
11	B	G	0	0	G	B	0	R	G	0	R	0	R	R	G	G	B	G	R	R	R	R	G	B	R	R	R	B	0	G	0	0
12	R	R	R	R	G	B	B	0	B	G	G	G	G	0	0	R	0	G	G	R	B	0	0	R	B	G	R	R	B	R	0	0
13	R	0	0	B	G	G	B	G	0	B	G	G	0	B	0	R	0	0	R	B	R	G	B	0	G	0	B	G	0	R	G	G
14	G	R	B	G	G	B	0	0	0	0	R	G	0	B	0	R	0	G	G	0	R	R	0	B	R	R	0	B	B	R	R	B
15	0	0	G	0	B	B	G	R	B	0	0	G	B	0	0	0	B	B	B	B	B	B	G	B	R	B	0	B	B	R	B	B	G
16	B	G	G	B	R	B	0	B	R	R	B	B	G	0	G	B	R	B	R	B	0	B	G	R	0	0	G	B	G	G	0	B
17	R	0	0	G	G	0	G	B	B	B	B	B	0	0	0	R	B	G	G	0	G	R	B	0	G	0	R	0	B	G	0	B
18	B	0	R	R	R	G	0	B	B	0	R	R	R	R	G	B	B	G	B	G	0	B	R	G	0	0	B	G	R	0	0	R
19	R	R	G	0	B	G	0	G	R	B	B	B	G	R	R	R	B	B	G	R	0	R	0	G	G	G	R	G	0	B	0	R
20	B	R	0	G	R	G	G	0	B	G	R	G	0	B	0	G	R	0	G	B	G	B	R	0	0	R	B	0	R	B	B	B
21	B	0	0	B	0	B	R	R	R	0	R	G	B	G	G	G	G	G	B	G	G	0	R	B	G	R	G	G	G	B	R	B
22	G	0	R	0	0	0	0	0	0	G	R	B	0	0	G	R	0	B	B	0	R	G	B	B	R	R	B	G	G	G	G	B
23	B	0	G	B	0	G	G	B	G	R	B	G	R	B	R	G	R	0	R	G	0	0	0	0	0	0	R	G	B	R	G	G
24	B	R	B	R	G	0	B	G	G	0	R	G	0	B	B	0	0	R	G	R	G	G	B	0	0	G	R	G	B	0	B	R
25	G	R	R	B	R	R	0	0	G	B	R	0	G	0	B	R	R	R	B	0	B	G	B	B	B	G	B	B	G	G	B	G
26	G	0	G	B	R	0	R	B	G	R	G	0	G	G	G	G	B	G	R	R	B	G	B	R	0	R	0	0	0	R	B	B
27	0	B	0	B	G	R	0	R	B	B	R	G	G	B	R	B	0	B	0	0	0	R	G	G	B	B	R	R	R	0	G	B
28	G	G	R	B	B	R	G	B	0	0	R	G	R	B	0	R	0	G	G	R	R	G	B	G	R	G	B	G	B	G	R	0
29	G	0	R	G	G	B	0	0	R	B	0	R	G	B	G	R	R	0	0	B	G	B	B	G	G	0	0	G	0	0	B	R	R
30	B	G	B	B	R	B	B	0	R	0	B	B	G	G	0	G	0	B	G	0	G	G	0	G	R	R	R	G	B	R	R	0
31	B	G	G	0	G	R	0	B	B	G	G	R	B	B	B	G	B	0	G	0	R	B	G	0	0	R	R	0	B	G	0	B

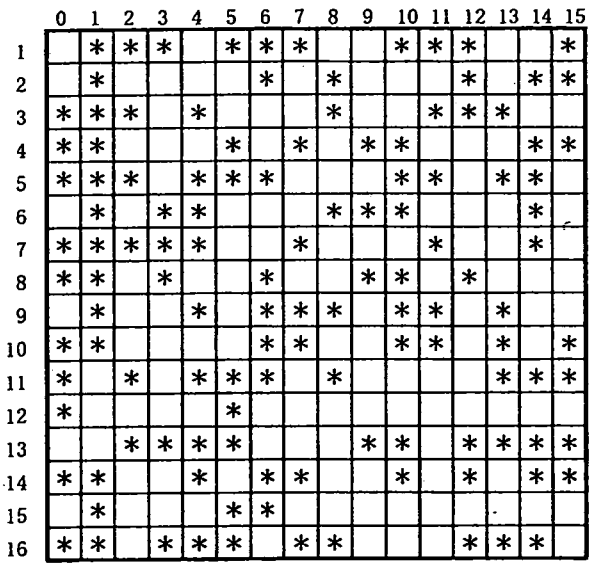
圖20



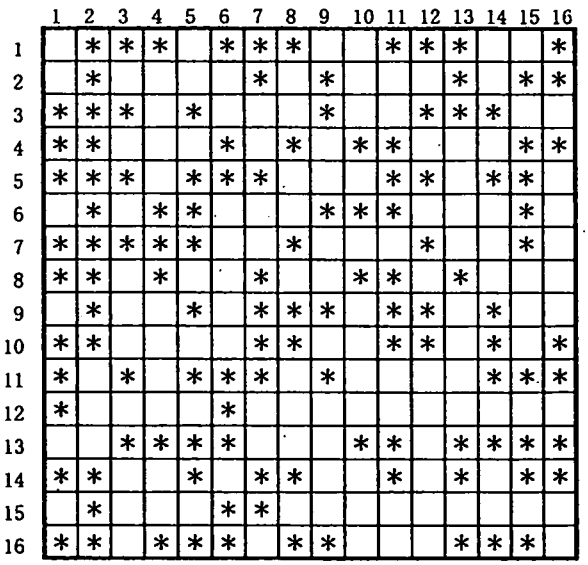
(a)



(b)



(c)



(d)

圖21

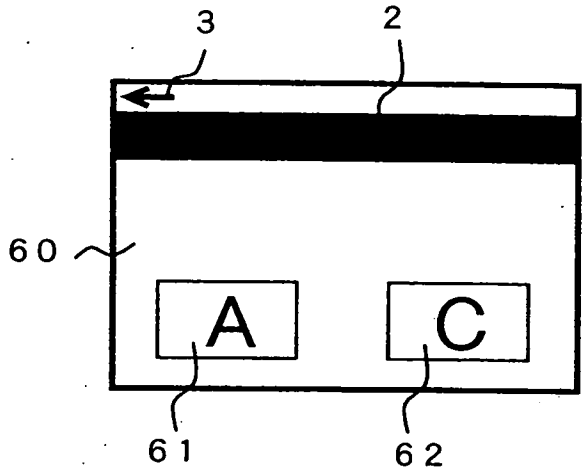


圖22

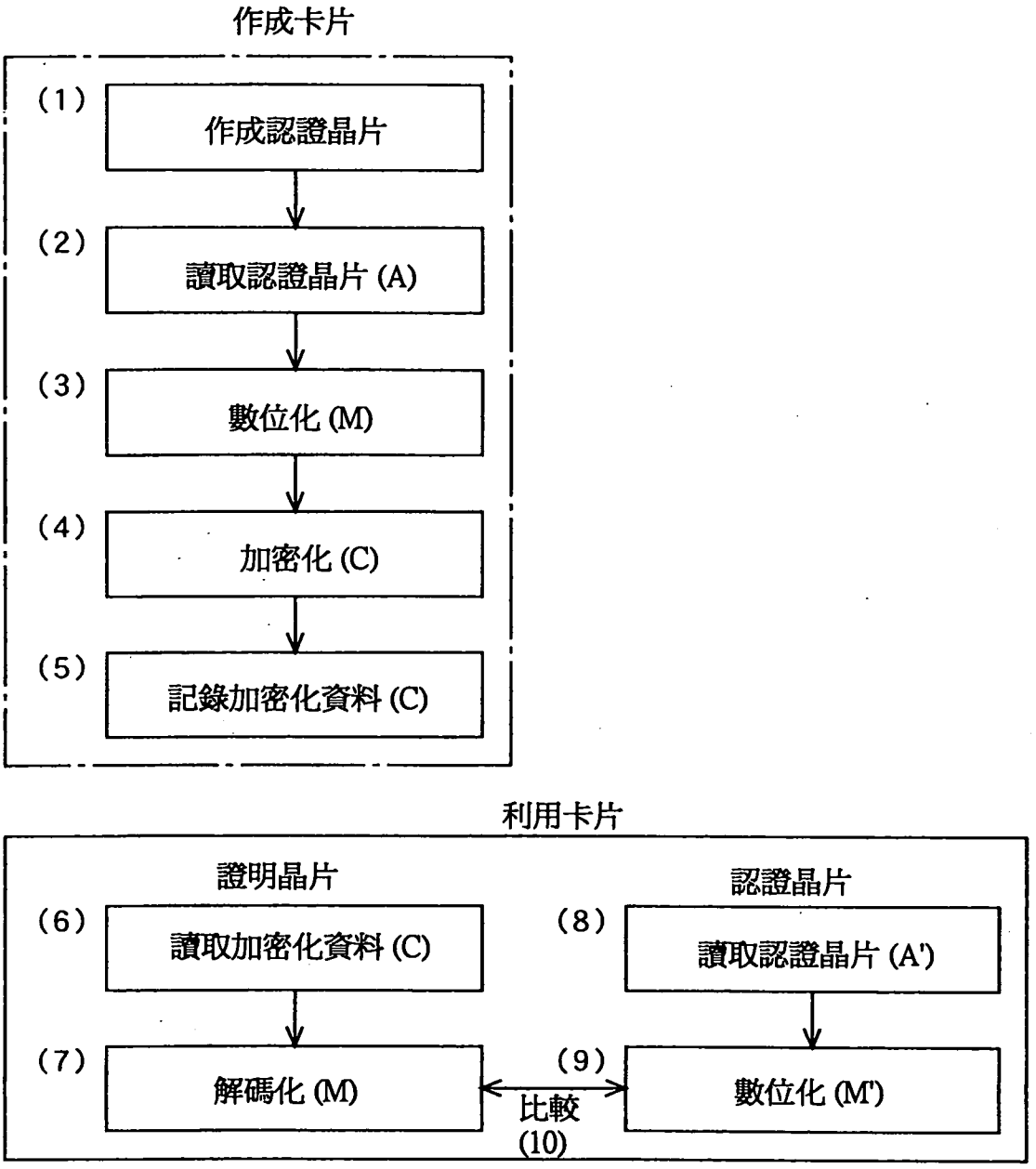

作成卡片
(1)
作成認證晶片
(2)
讀取認證晶片 (A)
(3)
數位化 (M)
(4)
加密化 (C)
(5)
記錄加密化資料 (C)
利用卡片
證明晶片
(6)
讀取加密化資料 (C)
(7)
解碼化 (M)
認證晶片
(8)
讀取認證晶片 (A')
(9)
數位化 (M')
比較
(10)

圖23

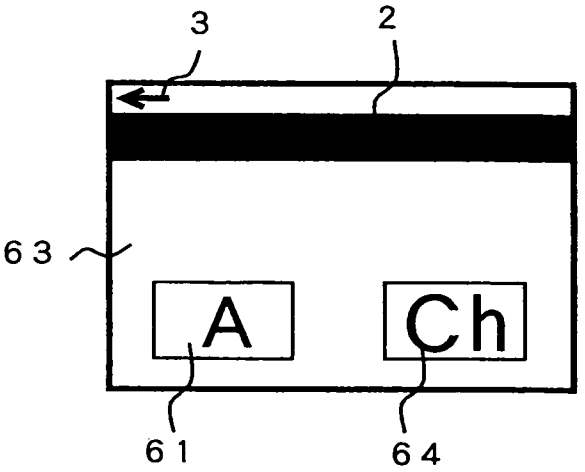


圖24

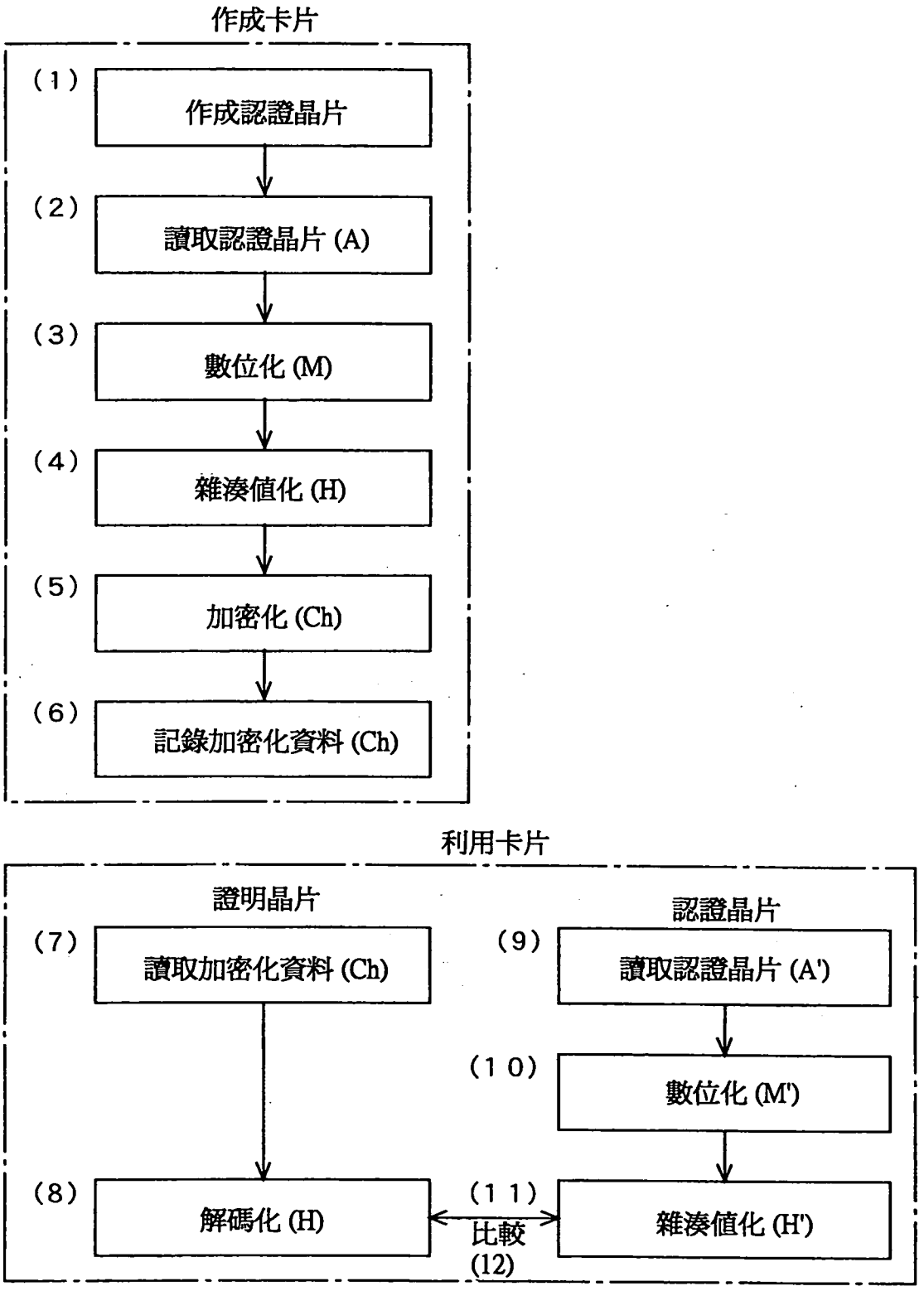

作成卡片
(1)
作成認證晶片
(2)
讀取認證晶片 (A)
(3)
數位化 (M)
(4)
雜湊值化 (H)
(5)
加密化 (Ch)
(6)
記錄加密化資料 (Ch)
利用卡片
證明晶片
(7)
讀取加密化資料 (Ch)
(8)
解碼化 (H)
認證晶片
(9)
讀取認證晶片 (A')
(10)
數位化 (M')
(11)
雜湊值化 (H')
比較
(12)

圖25

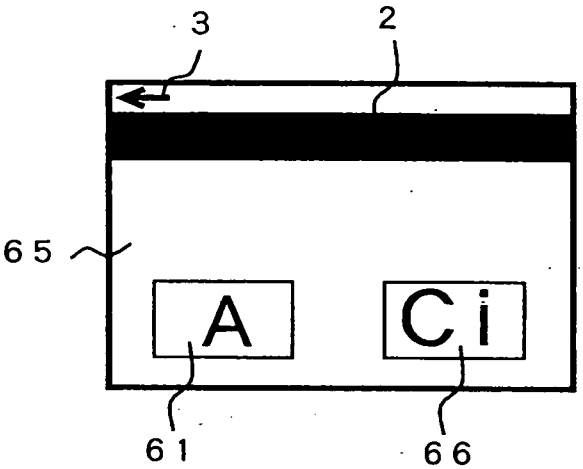


圖26

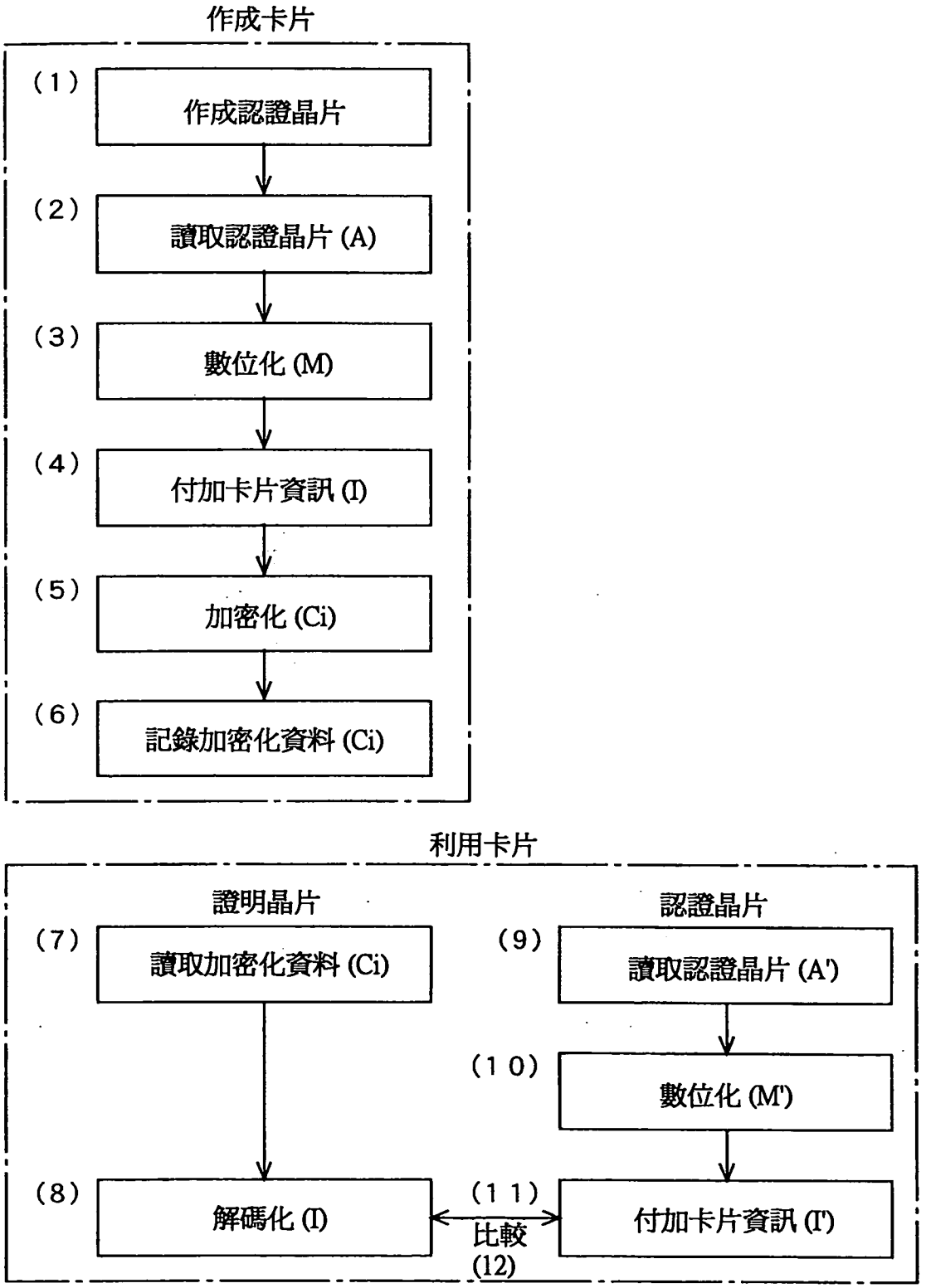
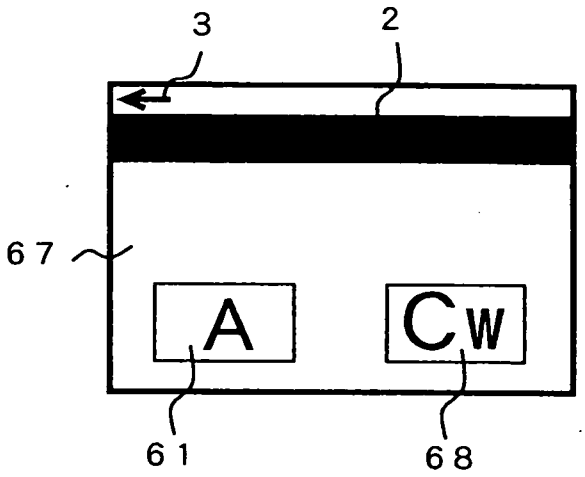

作成卡片
(1)
作成認證晶片
(2)
讀取認證晶片 (A)
(3)
數位化 (M)
(4)
付加卡片資訊 (I)
(5)
加密化 (Ci)
(6)
記錄加密化資料 (Ci)
利用卡片
證明晶片
認證晶片
(7)
讀取加密化資料 (Ci)
(9)
讀取認證晶片 (A')
(10)
數位化 (M')
(8)
解碼化 (I)
(11)
比較
(12)
付加卡片資訊 (I')

圖27



附件：第 95147699 號專利申請案
中文圖式修正頁　　民國 98 年 11 月 25 日修正

圖 28

98年11月25日修正頁

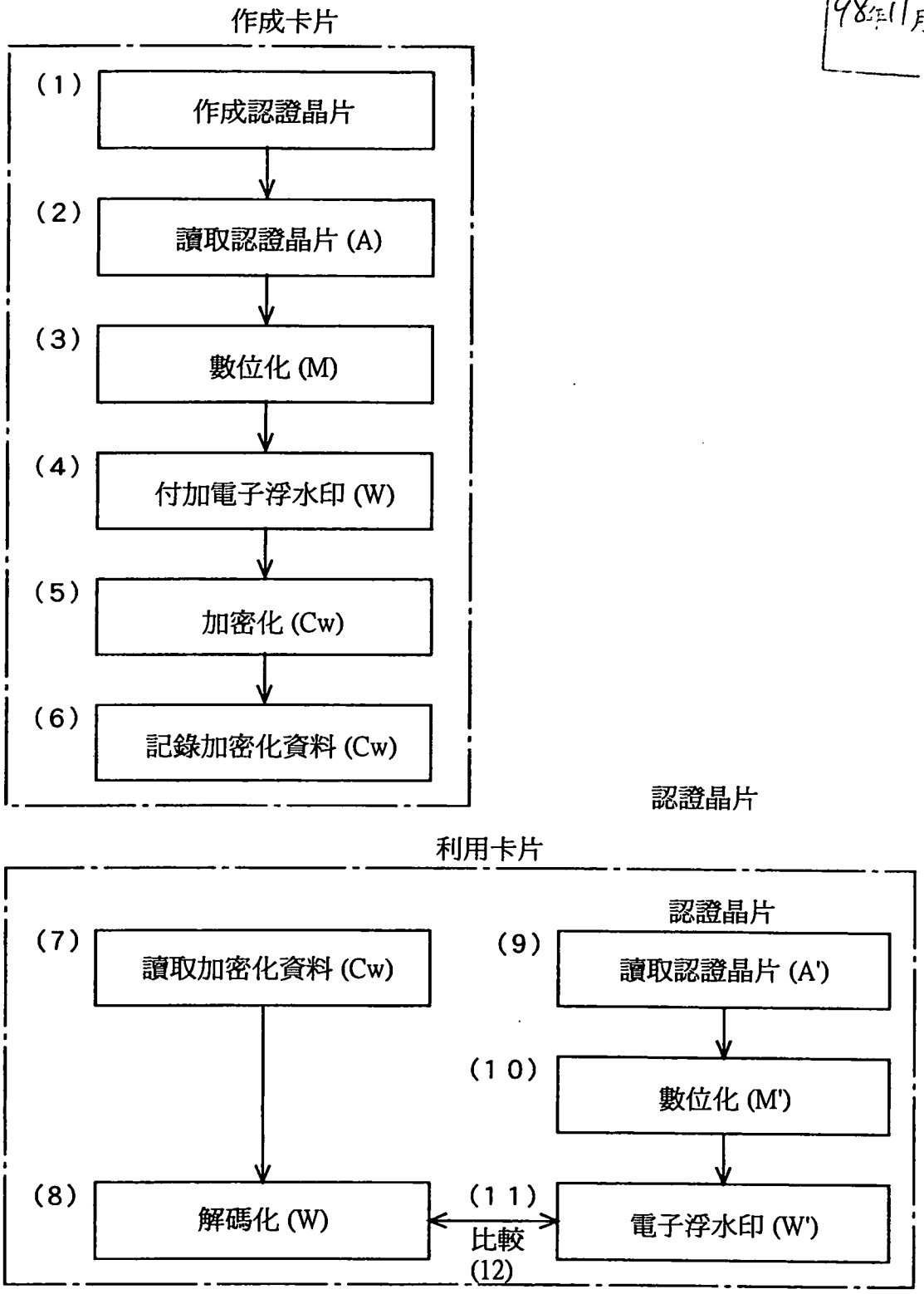


圖29

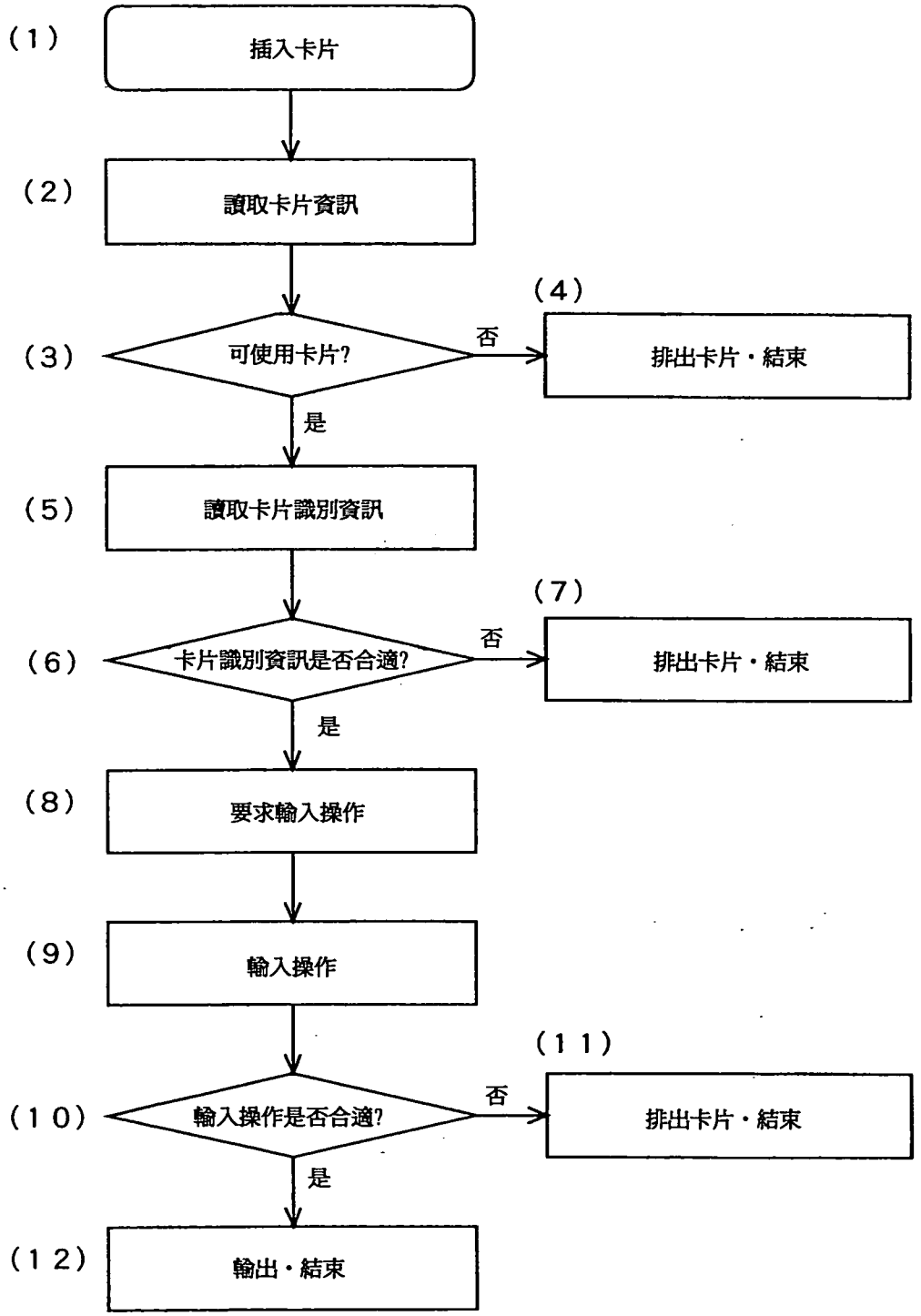

(1)
插入卡片
(2)
讀取卡片資訊
(3)
可使用卡片?
否
(4)
排出卡片・結束
是
(5)
讀取卡片識別資訊
(6)
卡片識別資訊是否合適?
否
(7)
排出卡片・結束
是
(8)
要求輸入操作
(9)
輸入操作
(10)
輸入操作是否合適?
否
(11)
排出卡片・結束
是
(12)
輸出・結束

圖30

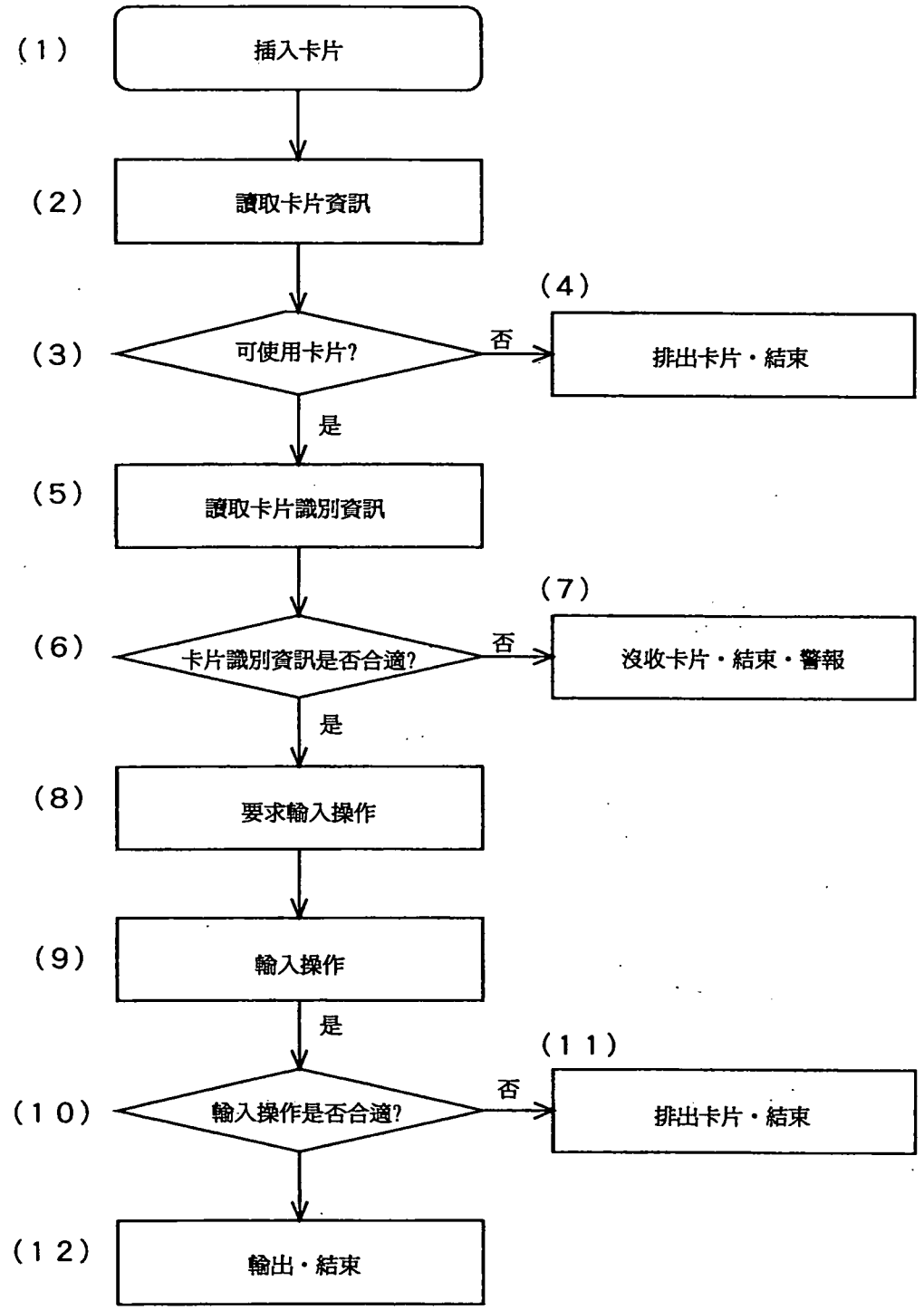
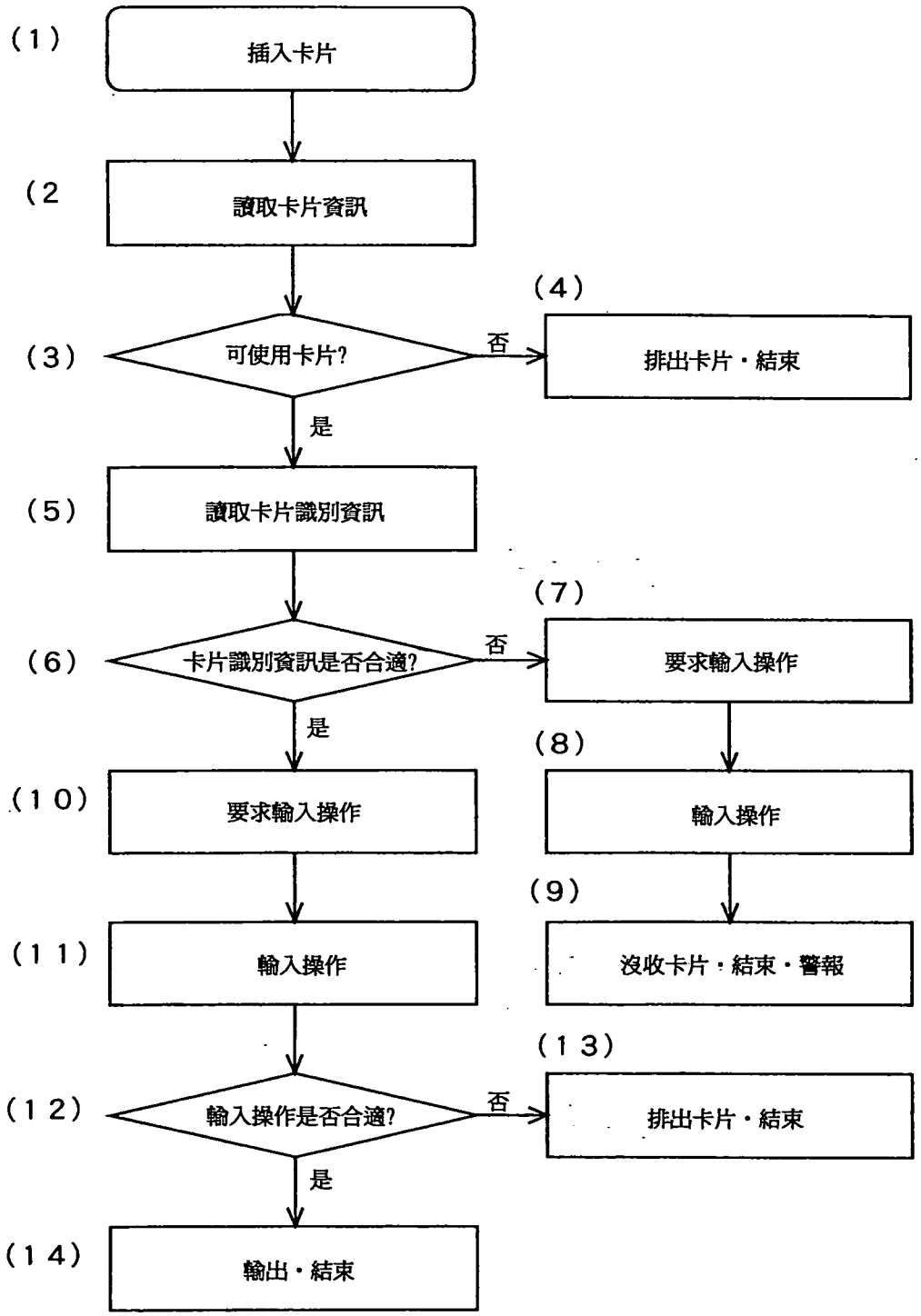

(1)
插入卡片
(2)
讀取卡片資訊
(3)
可使用卡片?
否
(4)
排出卡片・結束
是
(5)
讀取卡片識別資訊
(6)
卡片識別資訊是否合適?
否
(7)
沒收卡片・結束・警報
是
(8)
要求輸入操作
(9)
輸入操作
是
(10)
輸入操作是否合適?
否
(11)
排出卡片・結束
(12)
輸出・結束

圖31


(1)
插入卡片
(2
讀取卡片資訊
(3)
可使用卡片?
否
(4)
排出卡片・結束
是
(5)
讀取卡片識別資訊
(6)
卡片識別資訊是否合適?
否
(7)
要求輸入操作
是
(8)
輸入操作
(9)
沒收卡片・結束・警報
(10)
要求輸入操作
(11)
輸入操作
(12)
輸入操作是否合適?
否
(13)
排出卡片・結束
是
(14)
輸出・結束