200825968

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：95144900　　G06Q 30/00

※ 申請日期：95.12.4　　※IPC 分類：G06K 19/06

一、發明名稱：視覺秘密分享之行動電子票券系統

二、申 請 人：（共 1 人）

姓名或名稱：中華電信股份有限公司

代表人：賀陳旦

住居所或營業所地址：桃園縣楊梅鎮新榮里民族路五段 551 巷 12 號

國　籍：中華民國

三、發明人：（共 5 人）

姓　名：1. 白家榮

2. 藍元宗

3. 吳坤榮

4. 孫三為

5. 何業勤

國　籍：1～5. 中華民國

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係一種使用影像處理技術，將視覺秘密分享技術用在行動電子票券系統，可強化目前行動電子商務保密性及不可否認性等功能的視覺秘密分享之行動電子票券系統。

【先前技術】

現今市面上已有相當多地行動電子票券系統，所謂的電子票券，泛指將常用的文字訊息、一維條碼或二維條碼等條碼影像儲存於電子設備當中，而該文字訊息或條碼影像可代表任一商品資訊、電影票或大樓門禁鑰匙，該電子票券通常會有加密的動作，以防被他人竊取資訊或偽造。使用該票券時，可由一具有影像辨識能力的設備自動讀取電子票券資訊，使交易行為變的更加便利、迅速。其中文字訊息相當容易複製及偽造，是最不安全的電子票券形式。一維條碼及二維條碼雖然不易複製，但如果同時具有相對應的解碼器及編碼器，仍可以進行複製或偽造，對於經常接觸一維條碼及二維條碼的使用者而言，要知道是何種條碼形式相當容易，故其保密性仍是不足。因此上述系統無法提供較佳的保密性性，本系統為了克服上述系統的缺點，發明一視覺秘密分享之行動電子票券系統。

本案發明人鑑於上述習用交通監控系統所衍生的各項缺點，乃亟思加以改良創新，並經過多年苦心研究後，終於研發完成本件影像式交通監控系統，可與目前大部份的監控系統相結合，在

最少的花費下以達到最高的效能。

【發明目的】

本發明之主要目的即在於提供一種改良原本習用之系統，使其具有較高的保密性及不可否認性等特性的視覺秘密分享之行動電子票券系統。

【發明內容】

視覺式秘密分享和傳統式秘密分享的不同在於秘密重建的方法。傳統式秘密分享中秘密重建是使用電腦，而視覺式秘密分享中秘密重建是使用人的視覺系統。Naor 和 Shamir 在 1994 年提出了一個視覺式秘密分享的方法。他們的方法是將一個像素 P 可分成由兩個次像素所組成的兩個分解像素（s1 及 s2）。如果 P 是白色的像素，我們可以任意選擇圖一中前兩組分解像素的任一組。如果 P 是黑色的像素，我們可以任意選擇圖一中後兩組分解像素的任一組。由於 s1 一半是白色的，另一半是黑色的，因此由 s1 我們無法得知 P 是白色的像素或黑色的像素。同理，s2 一半是白色的，另一半是黑色的，因此由 s2 我們同樣無法得知 P 是白色的項素或黑色的像素。如果我們將 s1 和 s2 疊起來可以發現下列情況：如果 P 是黑色的像素，重疊起來的影像是黑色的，如果 P 是白色的像素則重疊起來的影像一半是白色的，另一半是黑色的。雖然 P 是白色像素的時候會有一半的對比損失，然而在視覺上依然可以分辨出來是白色的。這樣就可以達到秘密分享的目的。

本發明所提供之視覺秘密分享之行動電子票券系統主要由一

私密圖鑰產生模組、一公開圖鑰產生模組、一行動電子票券辨識模組及一私密圖鑰更新模組所組成，主要是將視覺秘密分享技術用在行動電子票券系統，加強電子票券系統的保密性及不可否認性。使用者使用時先於伺服器端建立一使用者帳號，並下載一私密圖鑰於行動設備（如手機或PDA），此私密圖鑰即為私密圖鑰產生模組所產生。接著在使用本發明所提供之視覺秘密分享之行動電子票券系統進行門禁通關或商務交易動作時，先由行動設備輸入使用者帳號，再與伺服器進行連線確認使用者身份，如果是合法使用者，伺服器會隨機產生一交易密碼，並依據使用者的私密圖鑰及通行密碼產生公開圖鑰並將之傳回客戶端。接著使用者欲使用此公開圖鑰時，行動設備的程式會將私密圖鑰及公開圖鑰疊合成一人眼可觀察的電子票券，利用具有行動電子票券辨識模組之設備將票券內容自動解碼，並與伺服器端進行確認該交易密碼是否合法，若是合法的交易密碼便完成此項交易。為了交易行為的安全性，使用者可隨時登入伺服器端更新私密圖鑰。

因此欲複製或偽造本系統之電子票券，只複製或偽造公開圖鑰時，無法得到合法的電子票券，需再具有使用者之私密圖鑰才能疊合出合法的電子票券，而本系統之私密圖鑰也只有使用者具有優先變更及下載的能力，因此具有相當高的保密性，也因為只有該使用者具有自己的私密圖鑰，才能疊合出具有合法交易密碼的電子票券，因此本系統也具有不可否認性。

【實施方式】

本發明「視覺秘密分享之行動電子票券系統」之客戶(Client)端及伺服器(Server)端之間之通訊協定說明如下：

客戶端	伺服器端
步驟一：輸入使用者識別名並傳送到伺服器端	
→	**步驟一**：接收使用者識別名 **步驟二**：檢查使用者識別名是否正確並傳送檢查結果到客戶端 檢查結果錯誤跳到**步驟三** 檢查結果正確跳到**步驟四**
步驟二：接收檢查結果 檢查結果錯誤跳到**步驟三** 檢查結果正確跳到**步驟四** **步驟三**：**結束**	←
	步驟三：結束 **步驟四**：讀取使用者私密圖鑰 **步驟五**：產生本次交易碼 **步驟六**：產生公開圖鑰 **步驟七**：傳送公開圖鑰到客戶端
步驟四：接收公開圖鑰 **步驟五**：結合公開圖鑰和私密圖鑰以產生電子票券 **步驟六**：利用電子票券辨識自動由電子票券得出交易密碼 **步驟七**：傳送交易密碼到伺服器端	←
→	**步驟八**：接收交易密碼 **步驟九**：檢查交易密碼是否正確並傳送檢查結果到客戶端 **步驟十**：結束
步驟八：接受檢查結果 **步驟九**：結束	←

申請私密圖鑰的流程如圖二所示：當動態交易密碼伺服器接到使用者帳號時，首先檢查此帳號是否合法，亦即在使用者資料庫中是否存在。如果是合法帳號，則檢查此帳號之私密圖鑰是否存在。如果不存在，則隨機產生私密圖鑰，否則詢問使用者是否

要更新該私密圖鑰或是取消動作。最後，將私密圖鑰存到使用者的行動裝置中，並將此私密圖鑰存入伺服器之資料庫中。

使用者驗證階段作業流程如圖三所示：使用者輸入使用者帳號後透過網路傳送至動態交易密碼伺服器。伺服器將檢查該帳號是否為合法使用者，以及該使用者之私密圖鑰索引是否存在。如果為合法使用者且存在相對應之私密圖鑰，則以一隨機亂數作為交易密碼，並根據此交易密碼以及私密圖鑰建立公開圖鑰。再透過網路將公開圖鑰傳送至使用者端與使用者端之私密圖鑰重疊得到人眼可見的電子票券。接著，利用電子票券辨識技術將電子票券所顯示之影像轉換為交易密碼，替代人工輸入。最後，如果使用者交易密碼正確，表示成功完成本次交易。另外，使用者可透過私密圖鑰更新方法同步更新使用者端之私密圖鑰以及伺服器端之私密圖鑰索引，以達到唯一私密圖鑰之目的。

本實施例所使用的電子票券為 QR Code，系統產生交易密碼後，可產生如圖四所示之電子票券，產生私密圖鑰的方法如下所述，首先為了使疊合後的電子票券長寬比例保持一致，因此本實施例所使用的分解像素如圖五所示，經由此分解像素亂數產生的私密圖鑰為圖六所示，相對應的公開圖鑰則為圖七所示，將私密圖鑰與公開圖鑰疊合後的電子票券如圖八所示。為了使辨識設備能順利將電子票券解碼出來，因此需要將疊合後的電子票券進一步清楚化，由於使用本實施例的分解像素，會使電子票券的白色

像素變成一具有 2 個黑點的 2×2 區塊，我們使用一簡單的清楚化方法，判斷疊合後的影像中每個 2×2 區塊，如果有 2 個以下的黑點，則將該區塊設定為白色區塊，否則將該區塊設定為黑色區塊，結果如圖九所示。

【特點及功效】

本發明所提供之視覺秘密分享之行動電子票券系統，與前述引證案及其他習用技術相比較時，更具有下列之優點：

1. 可加強行動電子票券之保密性。
2. 可增加行動電子票券之不可否認性。

上述詳細說明係針對本發明之一可行實施例之具體說明，若依本創作構想所作之改變，其產生之功能作用，仍未超出說明與圖示所涵蓋之精神時，均應包含在本創作之範圍內，合予陳明。

綜上所述，本案的確較習用物品增進上述多項功效，應已充分符合新穎性及進步性之法定新型專利，爰依法提出申請，懇請貴局核准本件新型專利申請案，以勵發明，至感德便。

【圖式簡單說明】

請參閱以下有關本發明一較佳實施例之詳細說明及其附圖，將可進一步瞭解本創作之技術內容及其目的功效；有關該實施例之附圖為：

圖一為本發明視覺秘密分享之行動電子票券系統之視覺式秘密分解像素示意圖；

圖二為該視覺秘密分享之行動電子票券系統之申請私密圖鑰

作業流程圖；

圖三為該視覺秘密分享之行動電子票券系統之驗證作業流程圖；

圖四為該視覺秘密分享之行動電子票券系統之實施例電子票券示意圖；

圖五為該視覺秘密分享之行動電子票券系統之實施例視覺式秘密分享方式示意圖；

圖六為該視覺秘密分享之行動電子票券系統之實施例私密圖鑰；

圖七為該視覺秘密分享之行動電子票券系統之實施例公開圖鑰；

圖八為該視覺秘密分享之行動電子票券系統之實施例含交易密碼之電子票券；以及

圖九為該視覺秘密分享之行動電子票券系統之實施例清楚化的電子票券。

【主要元件符號說明】

五、中文發明摘要：

一種視覺秘密分享之行動電子票券系統，其主要係於使用時先於伺服器端建立一使用者帳號，並下載一私密圖鑰於行動設備，此私密圖鑰即為私密圖鑰產生模組所產生，並在進行門禁通關或商務交易動作時，由行動設備輸入使用者帳號，再與伺服器進行連線確認使用者身份，如果是合法使用者，伺服器會隨機產生一交易密碼，並依據使用者的私密圖鑰及通行密碼產生公開圖鑰並將之傳回客戶端，且使用者欲使用此公開圖鑰時，行動設備的程式會將私密圖鑰及公開圖鑰疊合成一人眼可觀察的電子票券，利用具有行動電子票券辨識模組之設備將票券內容自動解碼，並與伺服器端進行確認該交易密碼是否合法，若是合法的交易密碼便完成此項交易。

六、英文發明摘要：

十、申請專利範圍：

1、一種視覺秘密分享之行動電子票券系統，其中包括：

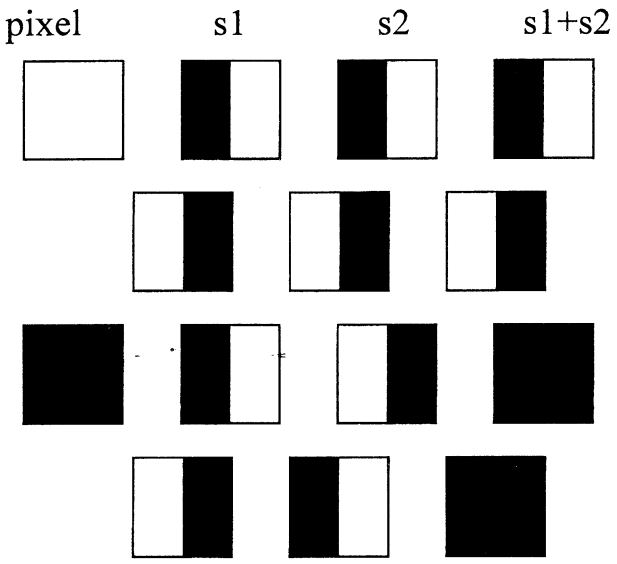
一私密圖鑰產生模組，該私密圖鑰產生模組依據自訂的分解像素隨機產生私密圖鑰，伺服器端將之傳送至使用者行動裝置並儲存於伺服端；

一公開圖鑰產生模組，該公開圖鑰產生模組會隨機產生一N位亂數的交易密碼，再轉換成任意形式的電子票券，並根據秘密分享原理，產生該電子票券與私密圖鑰相對應的公開圖鑰；

一行動電子票券辨識模組，該行動電子票券辨識模組先將私密圖鑰與公開圖鑰疊合之電子票券轉換成乾淨背景的電子票券，再利用影像辨識技術將電子票券轉換成N位數的交易密碼，轉換成乾淨背景的電子票券方法為每 2×2 區塊中判斷黑點的數量，若是區塊中黑點數量在 2 個以下，則該區塊中全部的點改為白色，否則區塊中全部的點改為黑色；以及

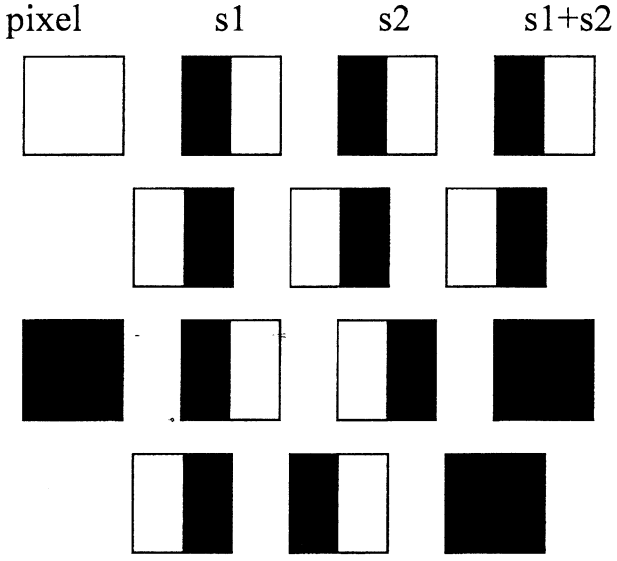
一私密圖鑰更新模組，該私密圖鑰更新模組可由使用者登入伺服器端，重新產生隨機的私密圖鑰，並將之同步更新伺服器端及使用者端的私密圖鑰。

十一、圖式：



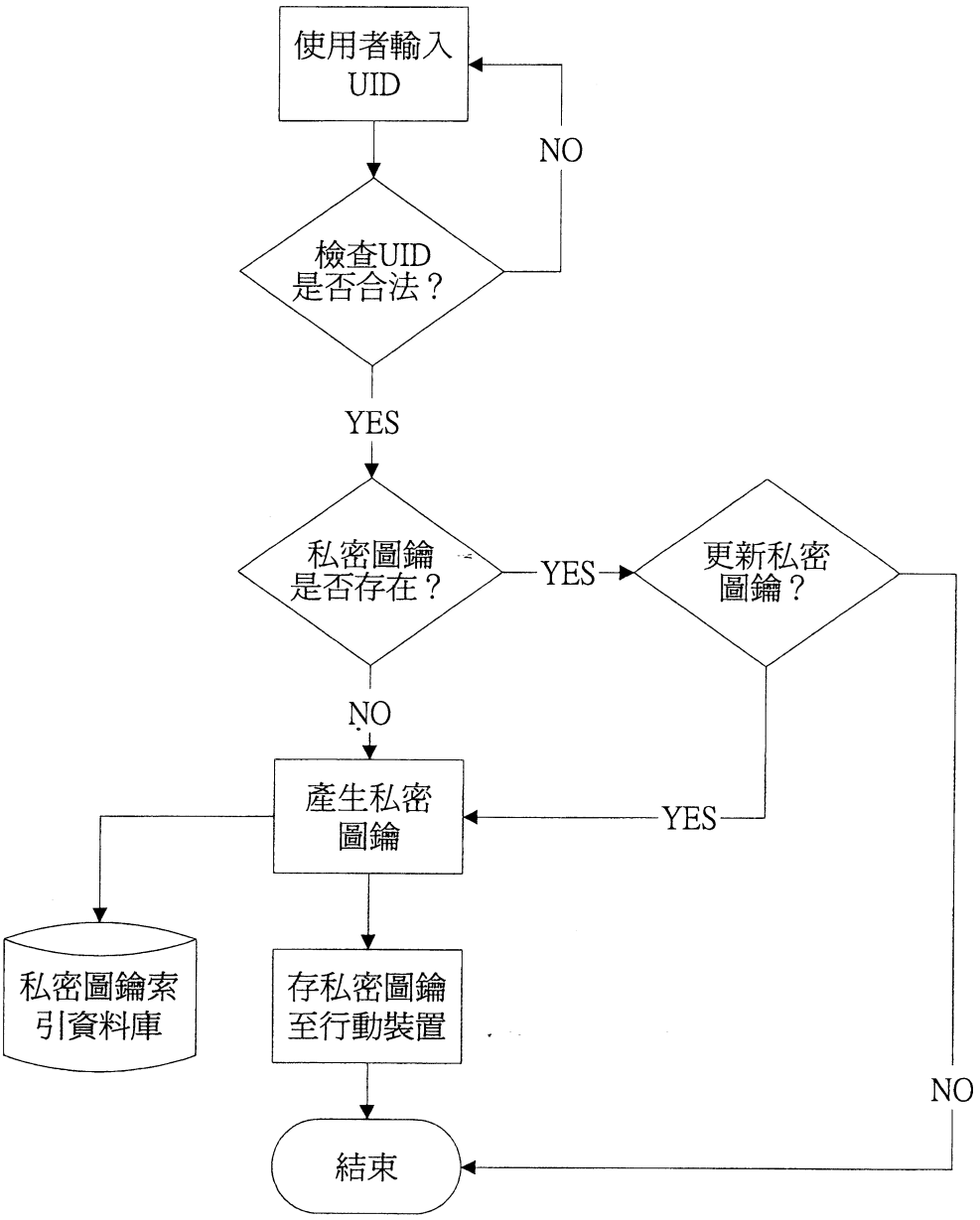
圖一

十一、圖式：



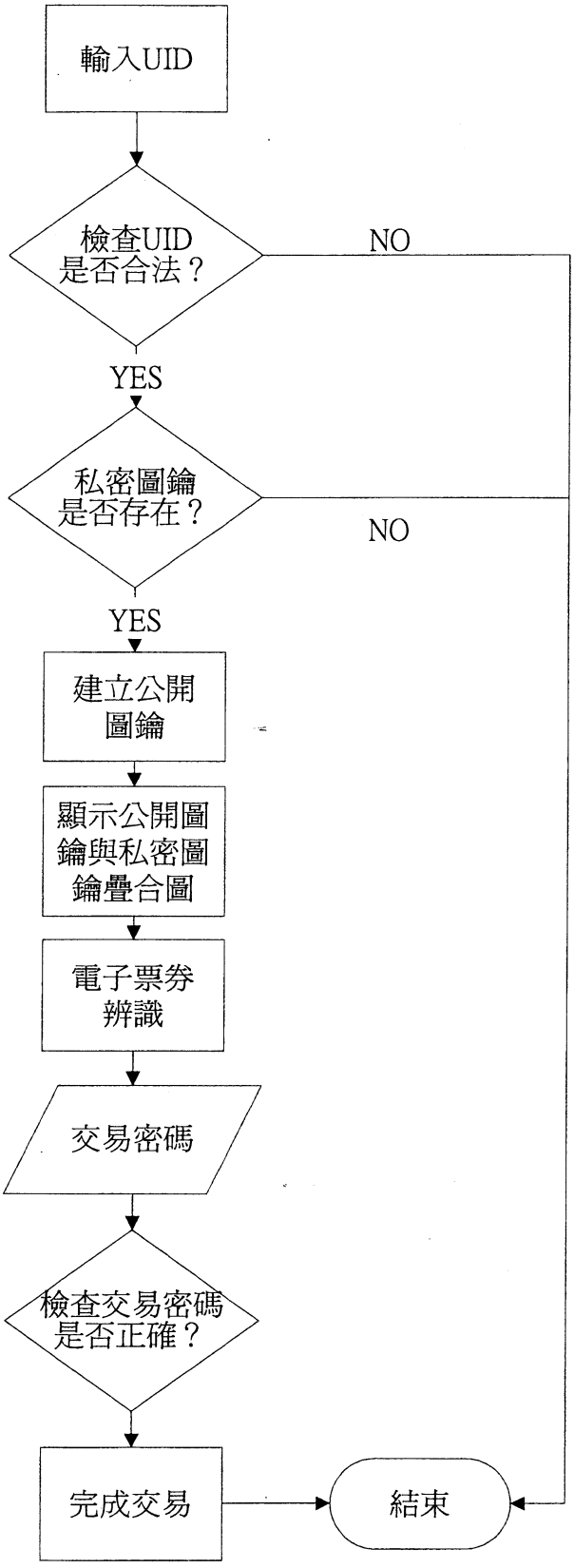
圖一

十一、圖式：


使用者輸入
UID
NO
檢查UID
是否合法？
YES
私密圖鑰
是否存在？
YES
更新私密
圖鑰？
NO
產生私密
圖鑰
YES
私密圖鑰索
引資料庫
存私密圖鑰
至行動裝置
NO
結束

圖二

十一、圖式：

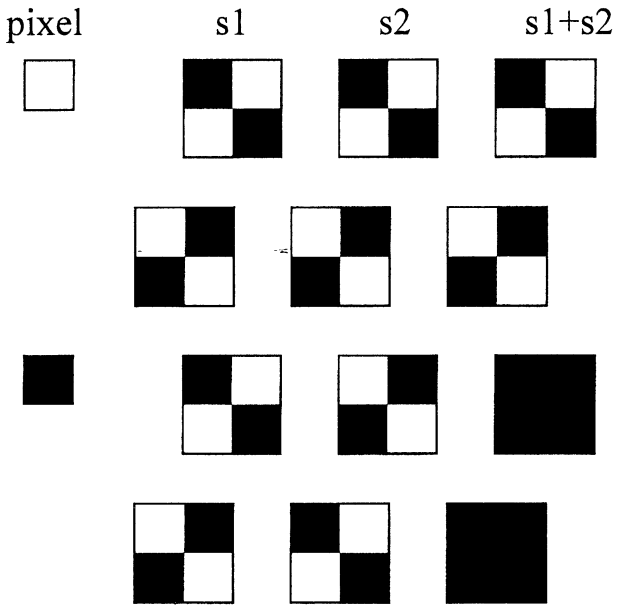

輸入UID
檢查UID
是否合法？
NO
YES
私密圖鑰
是否存在？
NO
YES
建立公開
圖鑰
顯示公開圖
鑰與私密圖
鑰疊合圖
電子票券
辨識
交易密碼
檢查交易密碼
是否正確？
完成交易
結束

圖三

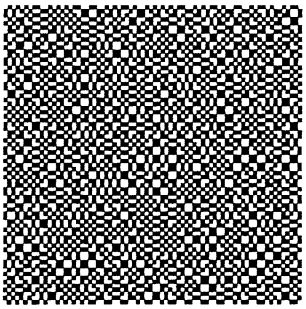
十一、圖式：



圖四

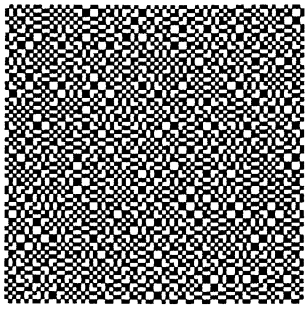


圖五

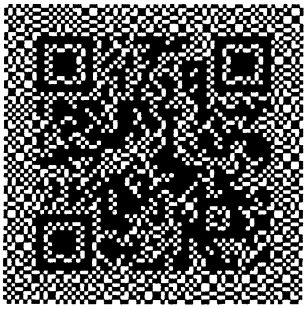


圖六

十一、圖式：



圖七



圖八



圖九

七、指定代表圖：

(一)本案指定代表圖為：第（　三　）圖。

(二)本代表圖之元件符號簡單說明:

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：