第二章、隨機點底紋影像之加密與驗證

在調幅網點中的藏密方式大抵透過調整網點位置、網點大小或形狀，而此加密後的變化易被識破，因而部份研究改以在隨機點分布的調頻網點中丟入零星的黑點或白點來達到藏密的目的，減輕藏密後所增加的破綻，但其中解碼時的影像對位就比較困難，對影像對位產生的誤差非常地敏感。而本研究中嘗試利用隨機點分布所構成整體幾何特性的資訊，同時達到加密與解密前的影像定位的特徵辨認。Vujovic and Brzakovic 的文件認證方法式針對已產生具有螢光絲底紋的文件進行隨機點辨認[23]，事先資料庫要儲存所有不同文件的資訊，而辨認過程中，以部分對應的方法解決影像對位的問題，並接續做文件真偽的判定；而本研究利用事先生成代表不同鍵值的隨機點圖樣，以旋轉、縮放與重疊等方式拼貼成產生加密影像，解碼時也利用部份對應的方法解決定位問題，而驗證時比對的對象換成了不同鍵值的基本密碼圖樣而非一張張的底紋影像，在儲存空間與比對過程的效率皆有優勢，另外應用上可以有更多的變化，例如產生不同序號的加密影像。

本研究提出利用隨機點分布的圖樣作為加密資訊，以其幾何轉換與部份重疊形成隨機點分布的網點影像(stochastic-dot texture)之方法，此加密影像在印列輸出後仍具有可供密碼認證的數位浮水印功能；而解碼驗證方面，因局部影像皆存在足夠的密碼訊息，利用電腦視覺中的部份對應方法，解決過程中可能產生的部分對應與幾何轉換問題，透過取像以及網點座標之偵測，本研究利用幾何雜湊法(Geometric Hashing)，比對攝取的特徵點與使用者宣告的金鑰值對應之隨機圖樣，當對應點超過一定數值，則認定此印刷品中有此基本隨機圖樣的存在，達到密碼驗證的目的。

2.1 隨機點圖樣

為有效節省密碼儲存空間與加速密碼驗證的時間，我們以隨機點分布形成基本密碼圖樣之幾何變換與部份重疊形成加密影像，使每小塊部分影像皆有足夠的訊息供作密碼驗證。隨機點分佈的密碼點可以利用亂數產生器產生或者由使用者自行設計，但圖樣本身必須具有隨機散亂的特性，以利在經過可能的幾何轉換後，還能與其他圖樣有鑑別力，在此提出一自動化的方式產生隨機點分布的方法，並考量在影像輸出後可能面臨的網點擴張問題造成鄰近點可能不易區分的缺點，加入一距離參數避免密碼點太過接近，如圖 2.1 的流程所示，欲產生 $R\times R$ 的隨機圖案，先以亂數產生器產生兩個 $0\sim R$ 的亂數分別代表密碼點水平軸 R_x 與垂直軸 R_y 的座標，如果該座標的周圍 d_1 的距離內沒有密碼點的存在時則紀錄該座標為密碼點的位置；否則重新產生隨機的座標。當密碼點數量達 m 個時則完成隨機密碼圖案，將此隨機密碼圖案儲存到資料庫並對應一鍵值紀錄之，以利後續進行密碼驗證時的比對，本研究中密碼點數量設為 50，密碼圖樣尺寸為 100×100，不同鍵值的密碼圖樣如圖 2.2 所示。以文件隨機圖樣底紋為例，隨機底紋的產生混合多個代表不同鍵值的基本密碼圖樣作為加密訊息，利用 S 個鍵值的基本密碼圖樣的排列組合搭配可以混合出最多 $C_{S/2}^{S}$ 種不同的編碼，例如本研究中所使用的 10 張不同鍵值的基本密碼圖樣可混合搭配出最多 252 種序號組合。混合多個密碼圖樣使編碼的複雜度提高也可避免有心人士利用部份對應的逆向工程將圖樣抓出。

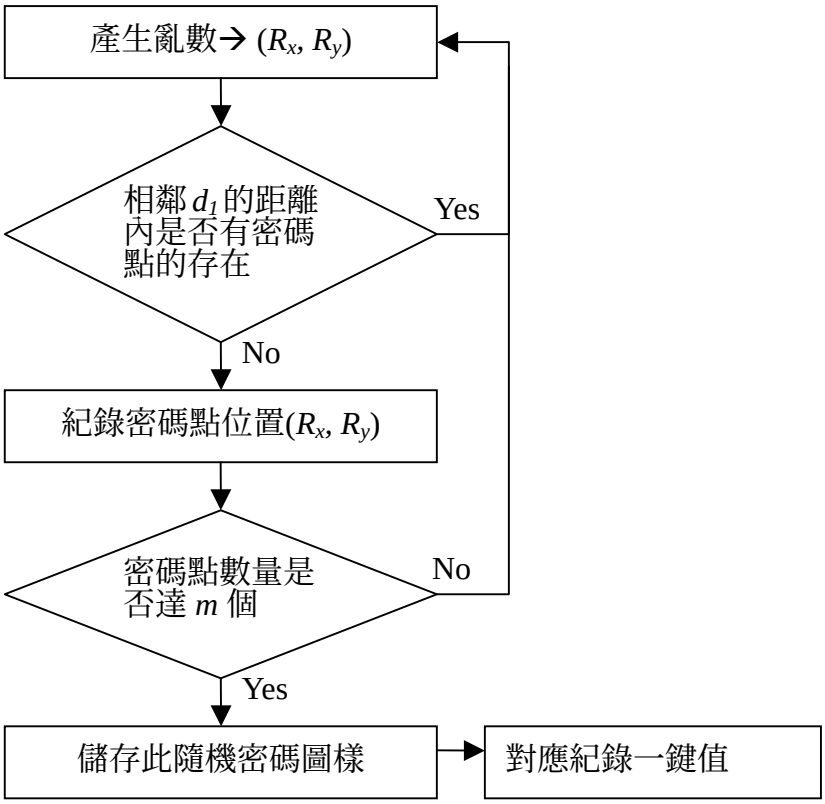


圖 2.1 隨機點圖樣產生過程

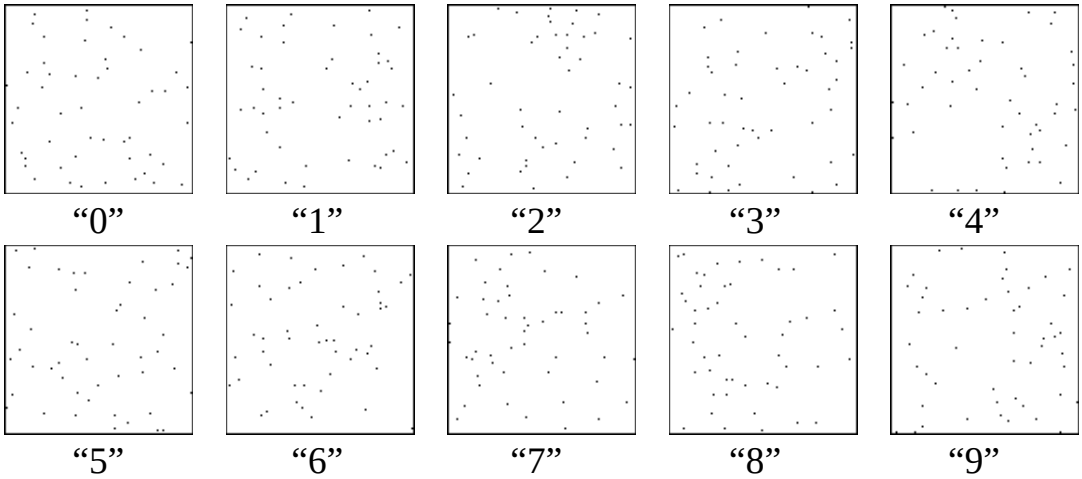


圖 2.2 代表不同鍵值之密碼圖樣

利用密碼圖樣之幾何變換與部份重疊產生隨機點分布的文件底紋。假設 $P_{k,m,0}$ 與 $P_{k,m,1}$ 分別為第 k 張密碼圖樣之第 m 個密碼點在 x 與 y 方向的座標值，密碼點數量總共 M 個。經方程式(2.1)的幾何轉換後得到密碼點的新座標值 $P'_{k,m,0}$ 與 $P'_{k,m,1}$， θ 為隨機旋轉角度，圖樣與圖樣間可有部份重疊的情形，如方程式(2.1)，使此圖樣可在一區間內隨機移動，在此設定 ε 為圖樣寬度的 20%。不論轉換過程中可能產生浮點數據，使轉換前後的點 P, P' 皆量化到最接近的整數值，以放置在數位影像中的像素位置。混合兩鍵值密碼圖樣之底紋影像如圖 2.3 所示，並印列輸出。

$$
\begin{aligned}
&\begin{bmatrix} P'_{k,m,0} \\ P'_{k,m,1} \end{bmatrix} = Rot_{2\times 2}\begin{bmatrix} P_{k,m,0} \\ P_{k,m,1} \end{bmatrix} + Trans_{2\times 1} \\
&where \quad m = 1,....,M \\
&\qquad Rot = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \\
&\qquad Trans = \begin{bmatrix} Tr_x \\ Tr_y \end{bmatrix}, \quad \{-\varepsilon \le Tr_x, Tr_y \le \varepsilon\}
\end{aligned}
\tag{2.1}
$$

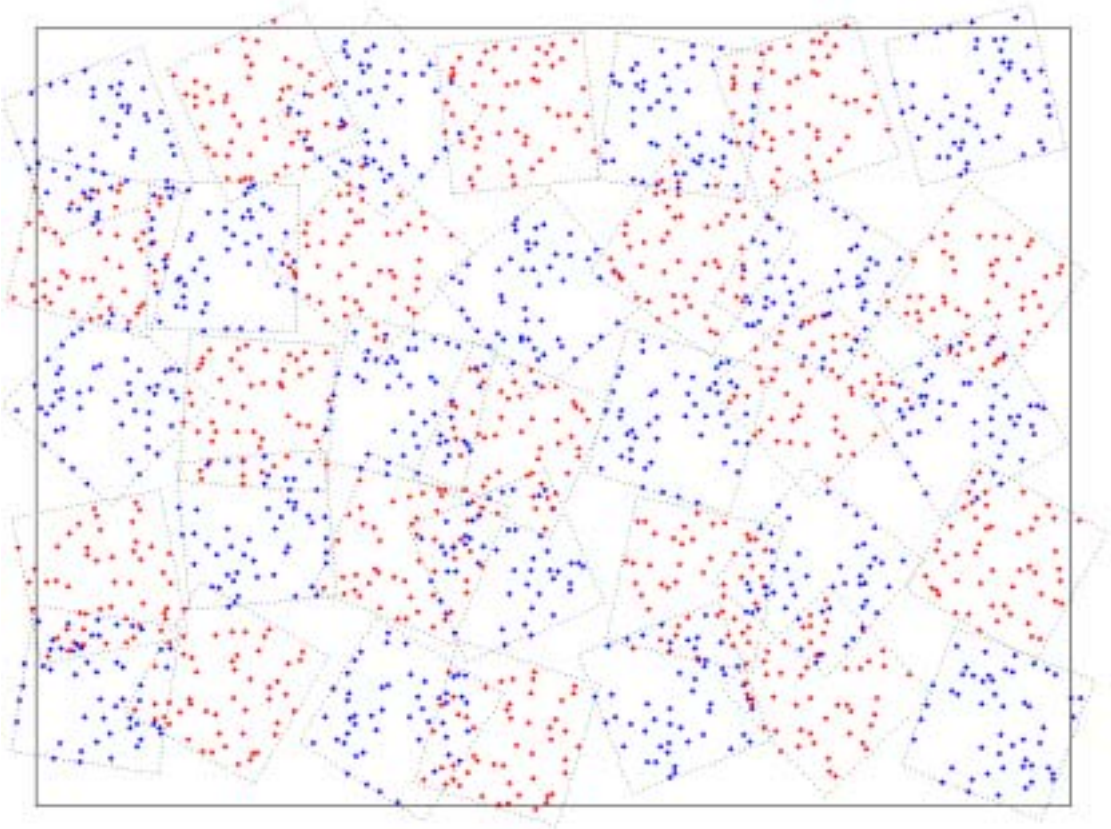


圖 2.3　隨機點底紋影像的產生，藍與紅分別代表不同鍵值

2.2 驗證方式

密碼驗證前要先攝取加密的底紋影像之數位影像，經萃取特徵值座標後，再以部分對應的方法解決影像定位之問題，本研究中使用幾何雜湊法解決影像定位之問題，在比對擷取影像中的特徵值座標與使用者宣告鍵值對應之密碼圖樣，若對應點超過一定票數則通過認證，驗證的流程如圖 2.4 所示。

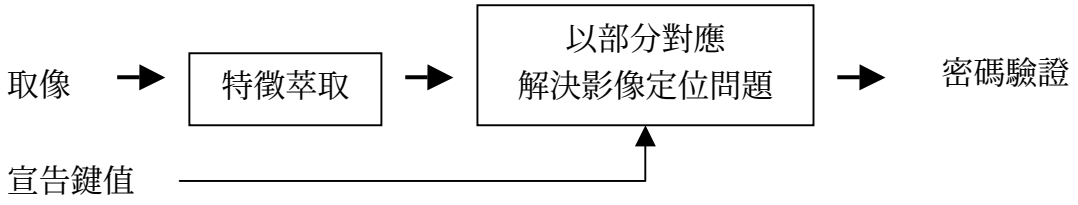


圖 2.4 印列輸出之加密影像的認證過程示意圖

2.2.1 特徵萃取

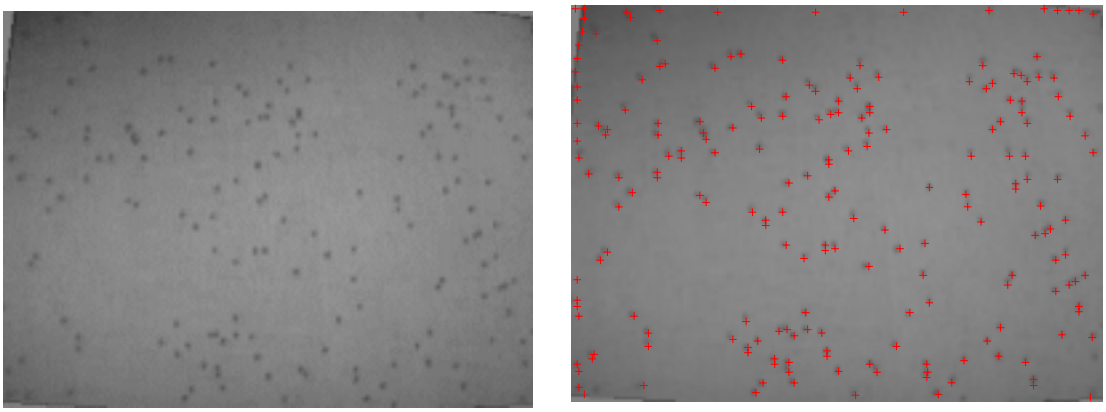
利用角點偵測萃取特徵值座標[7]，假設輸入影像為 I ，並取得其在水平與垂直方向的邊界影像 I_x 和 I_y，再者以高斯低頻濾波處理 $< >$將邊界影像作模糊化，並整理成一自相關矩陣 $\hat{C}$ 如方程式(2.2)。

$$\hat{C} = \begin{bmatrix} < I_x^2 > & < I_x I_y > \\ < I_x I_y > & < I_y^2 > \end{bmatrix} \tag{2.2}$$

$\hat{C}$ 主要的特徵向量代表邊界的走向，而其特徵值大小則反映出邊界的強度，兩個特徵值的大小可由方程式(2.3)表現。

$$R(x, y) = Det[\hat{C}] - \alpha Trace^2[\hat{C}] \tag{2.3}$$

$R(x,y)$愈大愈代表有角點的存在，而在其鄰近的區域的角點特徵也具有一定程度的顯著，因此選定一小視窗範圍 $w \times w$，當 $R(x,y)$的大於某一臨界值且在視窗範圍中為極大值，則確定座標(x,y)處有一角點存在，如圖 2.5 所示。



(a) (b)

圖 2.5 角點偵測萃取特徵點。(a)攝取的灰階影像；(b)紅色部分為偵測到的角點

2.2.2　以部分對應解決影像定位問題

過去針對具有浮水印的印刷品，常需對其重新取像得到數位影像予以解碼，而影像的自動校正定位在自動化解密是非常重要。常見的自動定位資訊是利用影像的四周邊界或四周的角點來校正影像，一但影像經裁切喪失定位資訊，解碼就變的非常有挑戰性，一張印刷品是由無數細小的網點所構成，為了區分外觀大同小異的網點，我們可以利用網點們所形成的幾何資訊來尋找定位資訊或與原密碼點間的對應關係。在尋找特徵點對應的過程，可能會因特徵點集合受部份遮蔽或雜訊的干擾，使特徵點消失或增加，這時可使用部分對應的方法進行比對。

電腦視覺中解決部分對應的問題已有系統化的方法應用於物件辨識(Object Recognition)。不論任何辨認方法都會分做兩階段：表示方式與比對方法。例如幾何雜湊法將物件的幾何轉換模型建立索引表表示之，再以統計的方式找出對應的幾何關係[13][25]；或是搜尋樹(Searching Tree)，將鄰近特徵值的幾何相關性建立成樹狀結構表示之，再作搜尋比對找出幾何關係[5][23]。此兩種方法在實作上各有優勢，在此使用幾何雜湊法顯示本研究在密碼驗證方面的能力。

2.2.2.1 幾何雜湊法

幾何雜湊法是 Lamdan 與 Wolfson 在 1988 年提出的以幾何不變量的座標表示法是輪流使用特徵點中的點子集合形成新的座標系[13][25]，將特徵點中的其餘的點集合投影到新座標系，儲存大量冗餘的座標系在資料庫中，當新進影像含有特徵點中的點子集合的話，則可在資料庫中找到相符合的座標系，以找到對應的幾何轉換關係。

欲比對新進影像中的特徵點集合 B 中是否有物件點集合 A 的存在，如圖 2.6 所示，以任兩點為基底以新座標表示作點對點的對應，在特徵點可能受到部分遮蔽或雜訊的影響有增減的情況下，還可找到正確的幾何轉換關係。幾何雜湊法提供在點集合 B 中重覆隨機指定基底與點集合 A 中所有可能的幾何模型進行比對，直到找到相對應的幾何模型，可定義一點對點對應的得票數門檻值作為證明在點集合 B 中有物件 A 的存在，例如圖 2.6 中對應的點有 4 點。

(a) (b)

圖 2.6 部分對應問題。(a)物件的點集合 A；(b)新進影像的點集合 B，特徵點可能受到部分遮蔽或雜訊的干擾而有增減的情形。

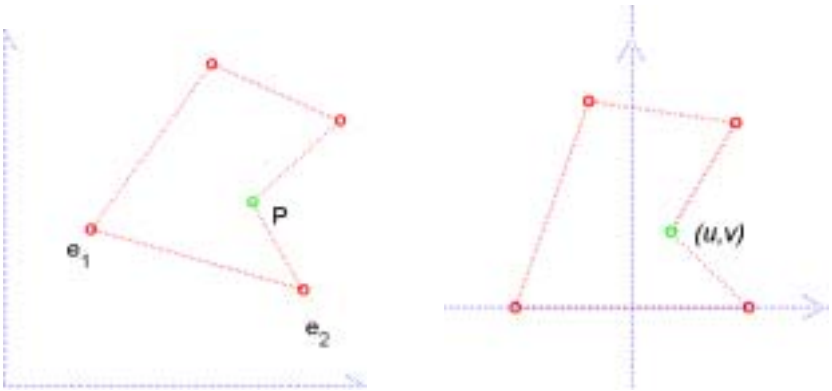
2.2.2.2 幾何不變量座標表示法

由於待測文件與掃描器或攝影機之間為相互平行的關係，因而只會造成平移與旋轉的的剛性轉換(rigid transformation)，如圖 2.7(a)所示，物件 A 本身有五的特徵點，當以 $\mathbf{e}_1$ 與 $\mathbf{e}_2$ 為基底時，$\mathbf{e}_1$ 與 $\mathbf{e}_2$ 之間的中點維新座標系的原點，此基底落在新座標系 x 軸上，其餘的點可以在新座標系上找到新的對應位置。以 **P** 為例，其在新座標系上的座標為(u, v)如圖 2.7(b)所示，可透過以下關係求得：

$$\mathbf{p} = u\mathbf{e}_x + v\mathbf{e}_y + \frac{\mathbf{e}_1 + \mathbf{e}_2}{2} \tag{2.4}$$

$$\mathbf{e}_x = \frac{\mathbf{e}_2 - \mathbf{e}_1}{\|\mathbf{e}_2 - \mathbf{e}_1\|} \tag{2.5}$$

$$\mathbf{e}_y = \mathbf{Rot}_{90}(\mathbf{e}_x) \tag{2.6}$$



(a) (b)

圖 2.7 將特徵點以新座標系表示。(a)原座標系；(b)以原特徵點中任取兩點為基底形成一新座標系

物件所有可能的幾何模型可以事先計算好存在資料庫中，並將其建立成索引資訊，以利加速比對。分別完成物件中的特徵點集合以兩兩配對點做為基底的新座標系，將所有特徵點座落在新座標系的座標值紀錄在以某配對為基底的模型中 Model(basic pair)，假設物件有 m 個基礎點，一共有 $m(m\text{-}1)$個模型。當處理到 **P** 點，其對應於基底為($\mathbf{e}_1$, $\mathbf{e}_2$)的座標為(u, v)，則在二維記憶陣列中(u, v)的記憶位置儲存 Model($\mathbf{e}_1$, $\mathbf{e}_2$)的資訊，如圖 2.8 所示。由於座標值(u, v)可能為浮點數，因此理想上希望記憶格子為無窮小。在實作上使用有限個記憶格子，每個格子可以記錄某一段範圍內的座標值，記憶格子的間隔為 r。記憶格子越小，座標表示越精確，但記憶量越大，也不容易克服雜訊的影響。記憶格子越大：座標表示越粗略，記憶量越小，較容易克服雜訊的影響，但之後的比對結果可能較不精確。

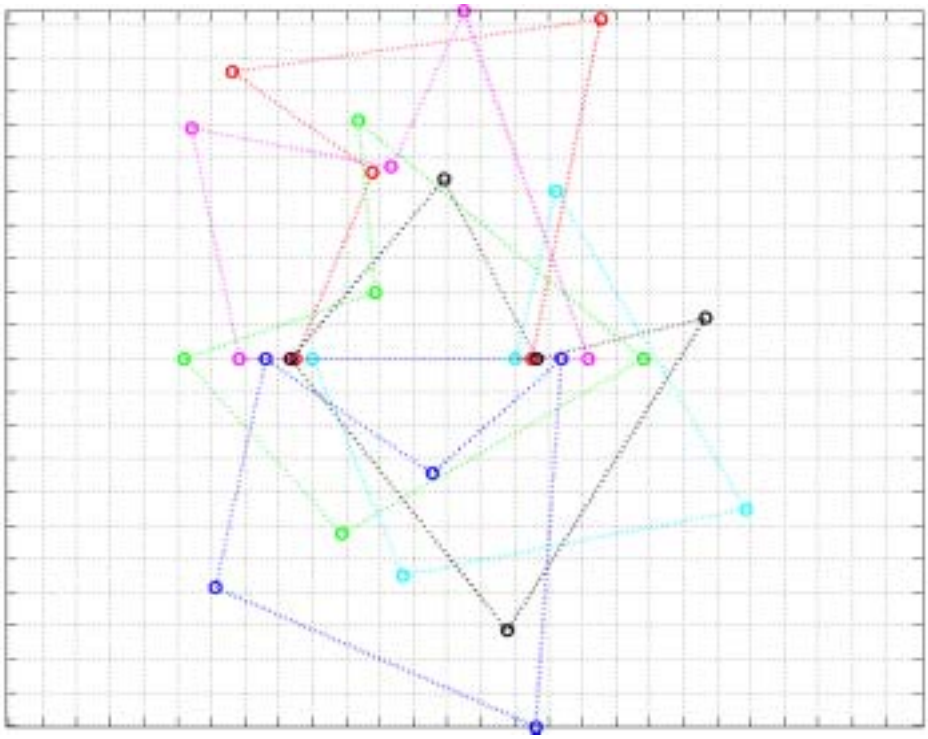


圖 2.8 不同的註記代表不同基底形成幾何模型

2.2.2.3　辨認階段

認證方式以幾何雜湊法作投票，當票數超過多少及認證為真；否則不通過認證。本研究的認證系統，事先取得使用者聲明所屬的金鑰值，並對應到一密碼圖樣。在離線端完成幾何雜湊表之後，在線上時執行密碼認證時，透過取像設備取得數位影像，並萃取特徵值座標後，任取兩兩配對的基底，將影像中的點集合轉換到新座標系，對資料庫中的該密碼的幾何模型作投票的動作，在依據幾個門檻值得到最後結果判定為密碼的真與否。為求系統速度與穩定，在有限次的隨機指定基底的幾何雜湊投票中，必須重覆對一鍵值比對成功達一定次數，才作最後的密碼確認，幾何雜湊法的驗證流程如圖 2.9 所示。

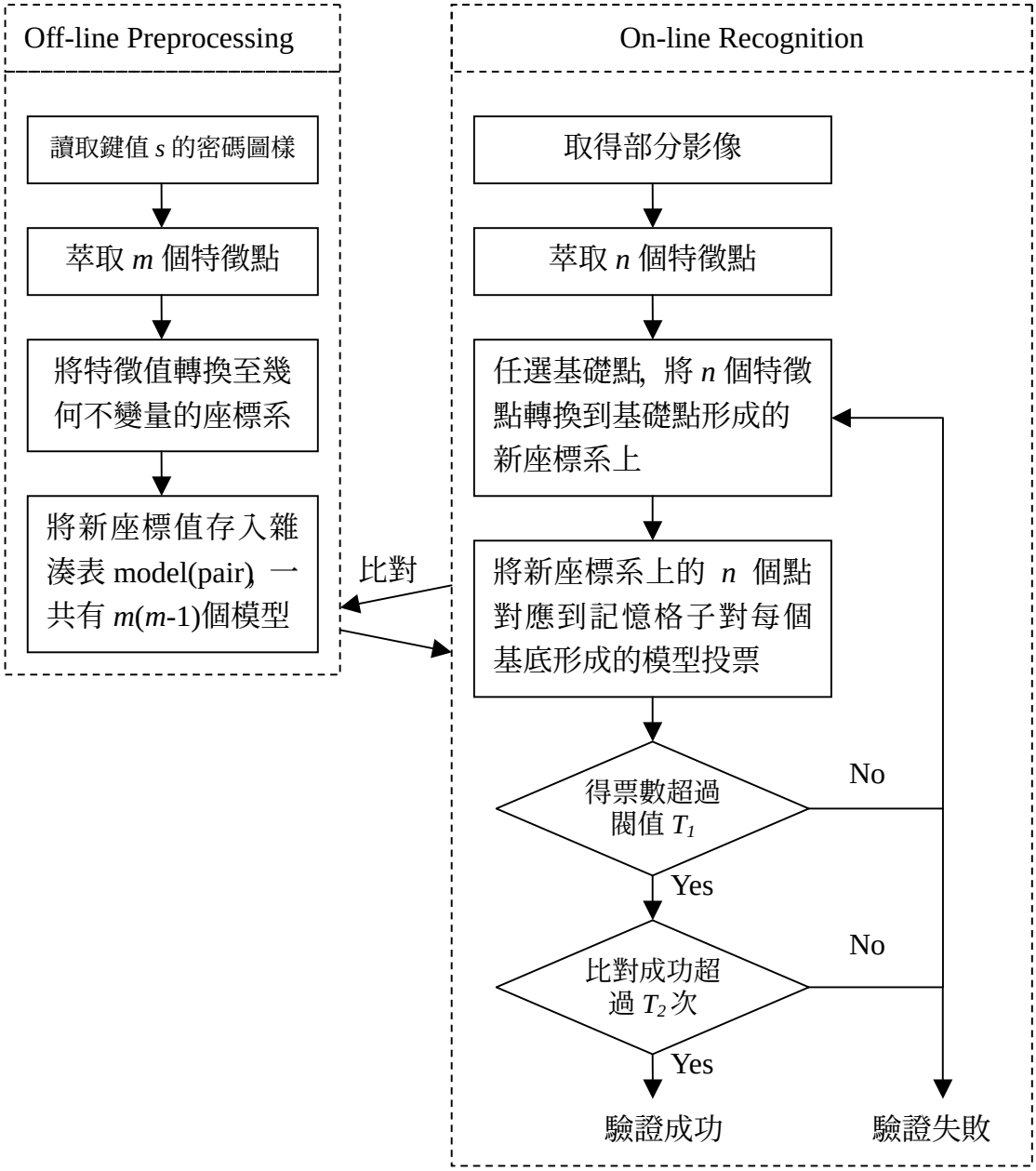


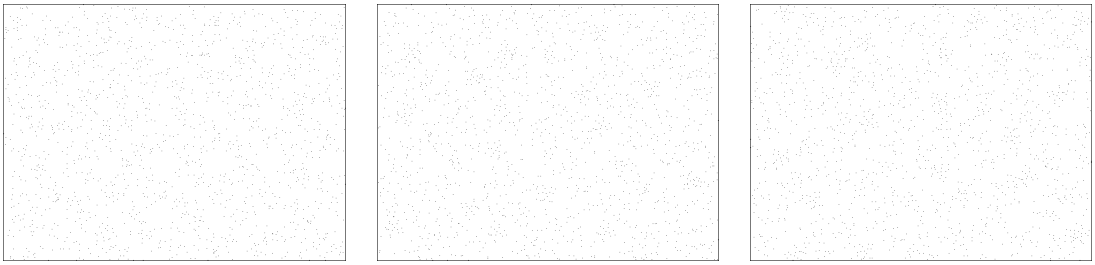
圖 2.9 使用幾何雜湊法之密碼驗證流程

2.3 訓練與測試

為因應實作上可能遇到的使用情況，以及適當參數的設定，本研究模擬使用情況的實驗，並找出適當的門檻值參數以因應實際狀態的需求，以下分作訓練與測試的敘述。

2.3.1 訓練

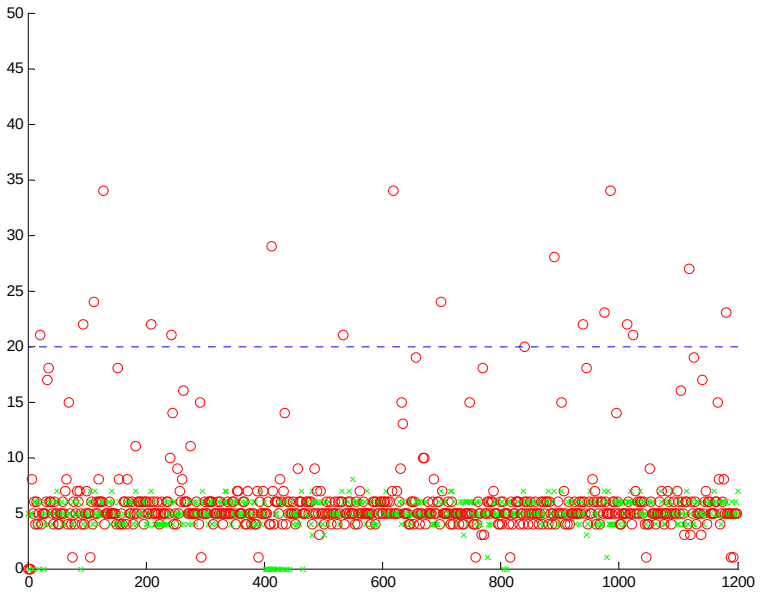
利用圖 2.2 十個不同鍵值的隨機點分佈的基本密碼圖樣之相互搭配，任取其中兩張密碼圖樣之隨機旋轉與部份重疊形成隨機點散布的底紋影像如圖 2.10 所示，分別以鍵值為“0”與“1”、“0”與“2”、“8”與“9”搭配形成的底紋影像為例，在外觀上無法以人眼區隔帶有不同密碼的底紋影像之差異，此三張底紋影像以影像解析度 360*dpi* 印列輸出作為訓練影像。



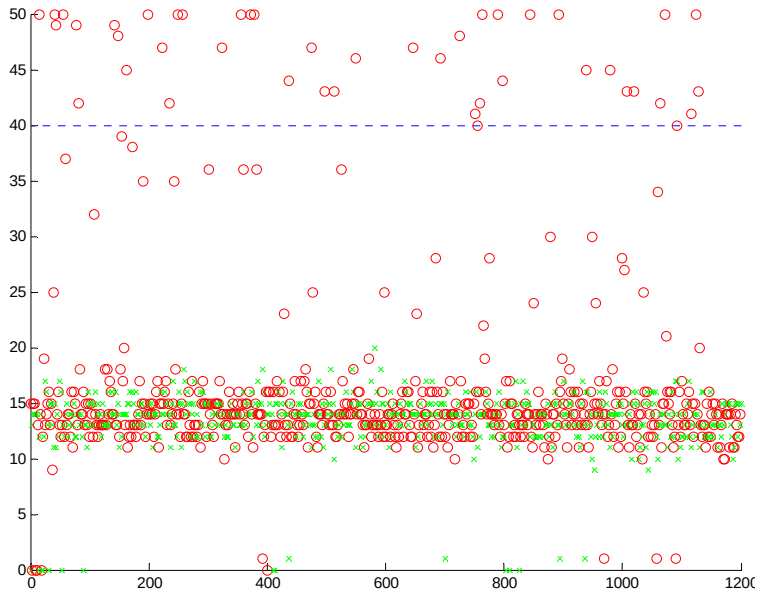
“0”& “1”　　“0”& “2”　　“8”& “9”

圖 2.10 搭配不同鍵值的密碼圖樣形成的底紋影像

以幾何雜湊法作為驗證工具，如圖 2.9 的流程，首先透過掃描解析度 720*dpi* 重建其數位影像，以利用角點偵測取得特徵值座標，以一次隨機選擇基底以及完成以下流程作為一次訓練程序，隨機選擇基底並將所偵測到的特徵點集合轉換到新座標系表示，再與使用者所宣告此張影像具有某鍵值的密碼圖樣之可能的幾何座標模型相互比較，將其中所得最高票的幾何模型之票數紀錄之。除了紀錄得票數外，如果此次比對的密碼恰為組成該底紋影像之密碼圖樣的其中之一的話，驗證鍵值與組成影像之鍵值相符則紀錄為“o”；不符則為“x”。在此幾何雜湊表的記憶格間距使用 1.5 像素，輪流取用三個底紋影像其中之一，對其中的特徵點集合隨機選擇基底，並以組成該底紋影像之某鍵值或任一不屬於組成成分之鍵值作為使用者宣告的密碼，利用提供機率各半的與組成影像之密碼圖樣相符的驗證鍵值或不符合的鍵值，進行模擬實際可能碰到密碼誤認之狀況。而反覆執行訓練程序 1200 次，每一次訓練程序包含一次隨機尋找基底，因而每次皆為獨立事件, 而 1200 次的得票數與比對結果如圖 2.11 (a)所示，預期票數越高者代表比對成功者，而希望密碼誤認的情形得到票數越低，圖 2.11 (a)中票數高的正例得票數大約在 10~35 票之間(密碼點數量為 50)與密碼誤認的反例票數大約在 10 票以下，在兩者判斷比對成功或失敗之間的得票數門檻值 T_1 設定 20 為恰當。然而在特徵值點集合對密碼圖樣之幾何模型投票時，比對成功者大部分若在記憶格子的鄰近區域，因而將鄰近九宮格的密碼點記憶格子納入投票的計算後，得票數高於未納入之前，如圖 2.11(b)顯示，得票數將近原圖樣的密碼點數量，且不易與其他金鑰的隨機圖樣混淆，所使用的比對結果得票數門檻值 T_1 設為 40 為恰當。爾後的在幾何雜湊投票過程中將落在雜湊點鄰近九宮格的票數一併納入計算，並訂定每次隨機指定基底對每一可能的幾何模型進行投票的票數必須超過 T_1 才為比對成功，T_1=40。



(a)



(b)

圖 2.11 幾何雜湊之密碼驗證的 T_1 門檻值之選擇。(a)每次模擬實驗所紀錄的票數；(b)將雜湊表鄰近九宮格的票數也納入計算之票數。橫軸代表實驗的次數，縱軸代表得票數

而在有限次隨機指定基底進行幾何雜湊的投票中，反覆比對成功越多次則可越確定在此輸入的影像中存有某鍵值的基本密碼圖樣，以使用者輸入其中之一訓練影像以及宣告的鍵值，在反覆 200 次中，每次將通過 T_1 的得票數視為比對成功，紀錄反覆成功的次數作為一次訓練程序。將使用者宣告的鍵值帶入符合或不符合組成該底紋影像之鍵值，提供機率各半的情況進行模擬實驗。當在有限的反覆次數中成功 T_2 次者視為驗證成功，如圖 2.12 所示，在此 T_2 訂定為 2.5 為恰當。

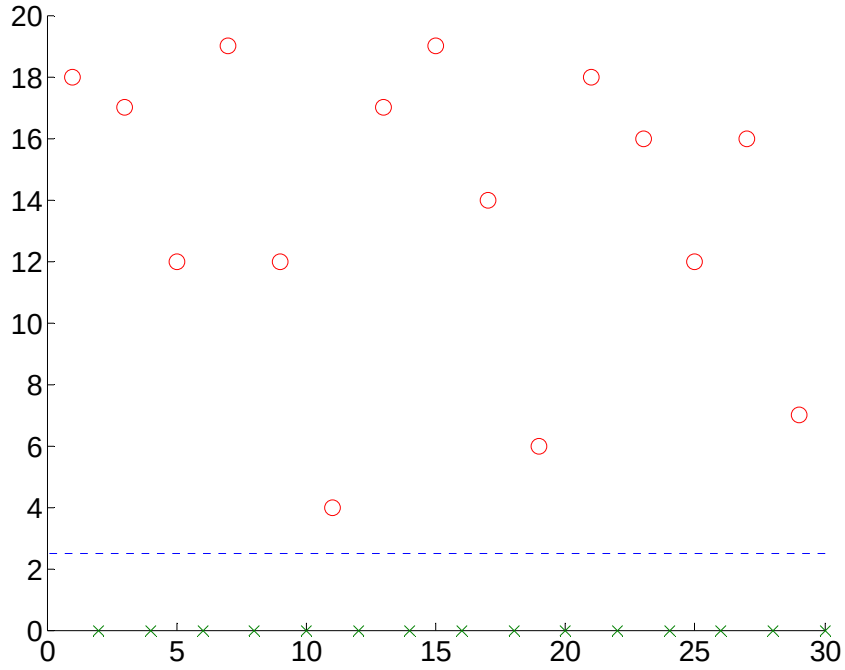
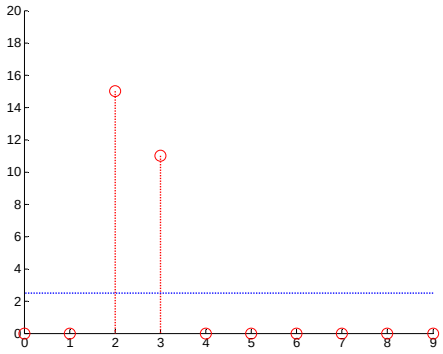


圖 2.12　有限次的隨機指定基底過程中，將比對成功次數 T_2 視為驗證成功。橫軸模擬實驗的次數，縱軸比對成功的次數

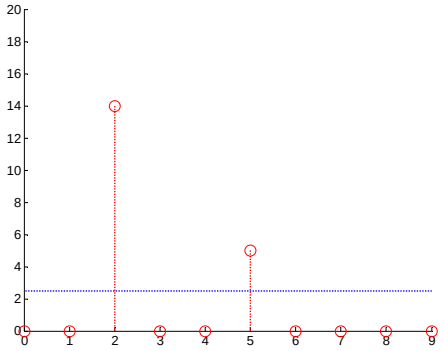
2.3.2 測試

利用圖 2.2 十個不同鍵值的隨機點分佈的基本密碼圖樣之相互搭配，任取其中至少兩張密碼圖樣之隨機旋轉與部份重疊形成隨機點散布的底紋影像作為測試影像，並以製作偽造的底紋影像，模擬實際遇到的攻擊狀況。底紋影像的組成至少具有兩個不同鍵值的密碼圖樣，而此鍵值即可代表此張影像的識別密碼，無法以人眼區別各別底紋影像之差異；實際情況可能碰到使用者拿偽造的影像企圖通過驗證，在此以隨機亂數產生類似的底紋影像(Fake I)，或者利用自行產生的基本圖樣之幾何變換與部份重疊形成類似的底紋影像(Fake II)。而這些底紋影像之尺寸大小皆設為 640×480，影像解析度設為 360*dpi* 印列輸出, 並以解析度 720*dpi* 掃描解析度重建其數位影像。

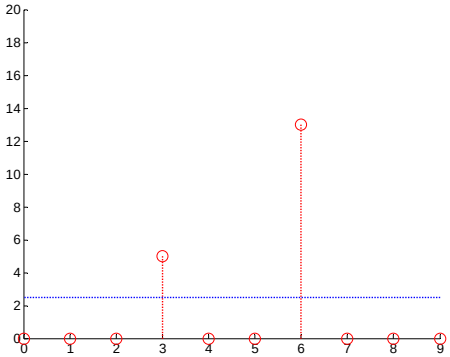
對每一數位影像進行角點偵測萃取特徵點座標，並隨機尋找基底，對某鍵值密碼圖樣作幾何雜湊的投票，當最高票者得票超過 T_1 視為比對成功，反之比對失敗。以反覆 200 次隨機尋找基底並與比對密碼圖樣比對的過程，反覆比對成功超過 T_2 次則視為驗證成功，反之驗證失敗，則完成驗證程序。宣告密碼圖樣之鍵值依序代入“0”到“9”進入驗證程序，並將反覆成功的次數與不同鍵值之對應以圖 2.13 表示之。



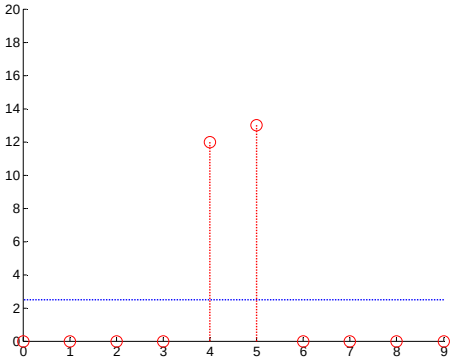
“2”&“3”



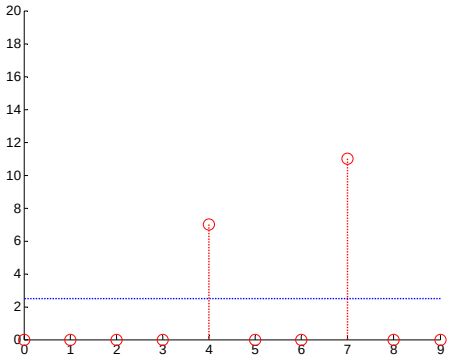
“2” & “5”



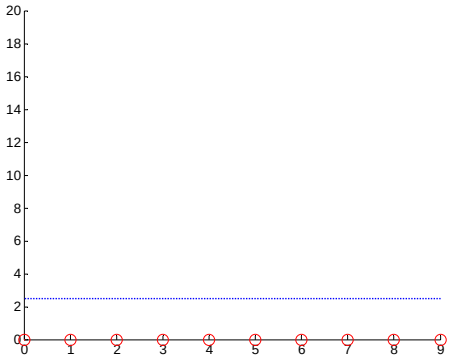
“3” & “6”



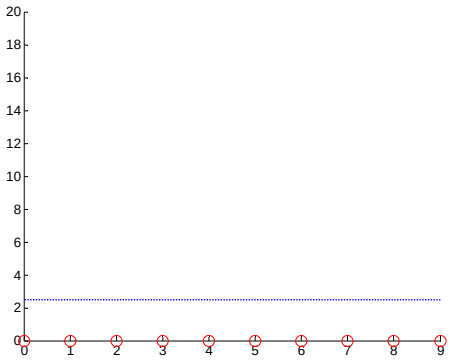
“4” & “5”



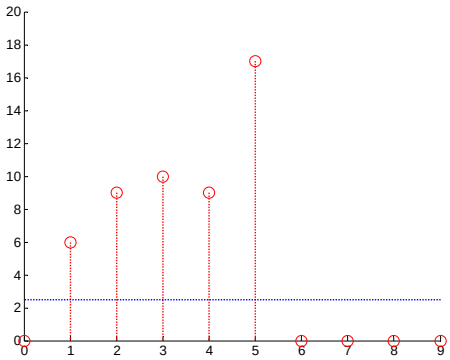
“4” & “7”



Fake I



Fake II



“1”,“2”,“3”,“4” & “5”

圖 2.13　對不同鍵值構成的底紋影像之驗證結果

以上利用基本密碼圖樣的隨機旋轉、平移與部份重疊形成隨機點分布底紋影像，看似難以用人眼去區別；而且每張底紋影像混合兩種以上的基本密碼圖樣，不同鍵值間不會造成誤判，則可作為不同的序號供不同使用者使用；並可以防止有心人士以偽造底紋影像企圖通過認證。