第三章、以網點為基礎的創新影像加密技術

除了以前一章節以隨機旋轉與部分重疊的方式形成無意義的底紋影像之外，在此我們利用基本密碼圖樣的縮放變化呈現不同階調以形成具有意義的影像。不同縮放尺度下的基本密碼圖樣在單位區域中的密碼點數不同，因而可變化不同濃度，以模擬影像的層次感，而此種方法同時達到影像加密與將灰階影像半色調的目的，由於影像中的每一細節皆由基本圖樣的幾何轉換所構成，則可利用部分對應之方法對任意的局部影像達到密碼驗證的目的，同時隨機點分布的基本圖樣在幾何轉換以及部份重疊後在視覺上仍具有隨機性，無法以人眼破解密碼。加密後的影像如圖 3.1 所示，整體呈現隨機點分布的半色調影像，微觀處的網點以隨機散亂的呈現，卻有密碼圖樣隱藏在其中。

圖 3.1　加密後的影像呈現隨機點分布的半色調影像

由圖樣中的密碼點在不同縮放尺度之下，將同樣區域中點數的增減情形，藉以呈現 N 種階調變化的情形，如圖 3.2 的示意，將圖樣縮至最小呈現最深的階調，圖樣放大可以呈現較淡的階調，以及利用全白的圖樣呈現最淡的階調。以此不同的縮放尺度的圖樣進行影像的描繪，由淡化到濃的步驟，先以全白的圖樣作為最淡階調的白色畫布，再以放大的圖樣描繪影像中呈現較淡的階調，以此類推，將不同縮放尺度的圖樣作為模擬影像階調的筆刷，慢慢畫到最深階層，在此由淡畫到濃的過程，也由於階調淺的筆刷大於階調深的筆刷，而具有從粗糙畫到細緻的意涵。

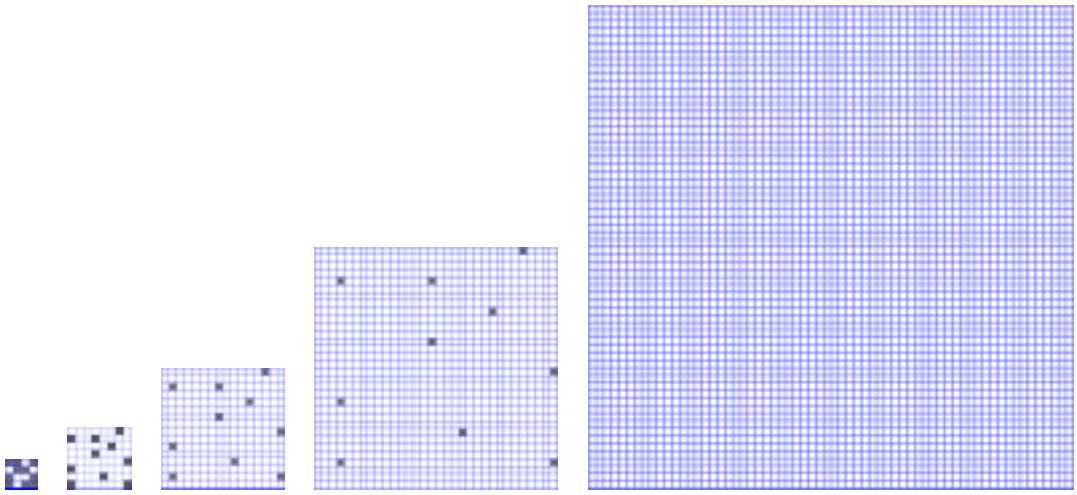

圖3.2 不同縮放尺度的基本密碼圖樣可呈現出不同濃度階調

3.1 影像分層

在此以圖樣的縮放產生有限的階調將原灰階影像劃分成 N 階層，本研究中以 N=5，以圖樣四個尺度的縮放與純白底色將灰階影像以五階層呈現，每階層影像 L_ℓ {0,1}如方程式(3.1)求得，由淡到濃分別為 L_0, L_1, L_2, L_3, L_4，如圖 3.3，如圖 3.4 所示以五階調表現影像。

$$L_\ell(i,j)=\begin{cases}1, & (\mathrm{N}-\ell-1)\times\dfrac{255}{N}<I(i,j)\le(N-\ell)\times\dfrac{255}{N}\\ 0, & otherwise\end{cases} \tag{3.1}$$

$$where \quad \ell=0,1,2,3,4$$

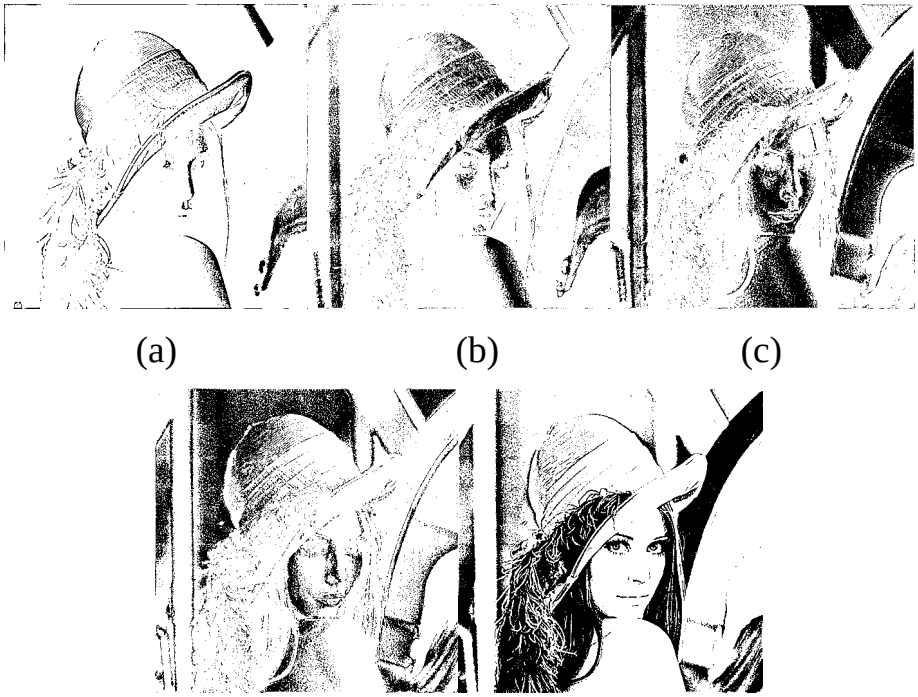

圖 3.3　由淡到濃分別為 L_0, L_1, L_2, L_3, L_4。

圖 3.4　影像分層五階調，由淺至深分別以白、藍、綠、紅、黑代表

3.2 以圖樣的縮放形成不同階調

利用密碼圖樣內密碼點在幾何上的縮放，形成不同大小的圖樣，以生成不同階調以模擬影像的層次感。假設 $P_{k,m,0}$ 與 $P_{k,m,1}$ 分別為鍵值 k 的密碼圖樣之第 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(3.2)的幾何轉換後得到密碼點的新座標值 $P'_{k,s,m,0}$ 與 $P'_{k,s,m,1}$，其中 s 為縮放尺度，在此設定 s=0.25, 0.5, 1, 2，以得到縮放後的圖樣作為影像繪圖筆刷，在繪製影像的過程中，如同圖 2.3 的拼貼方式在同一縮放筆刷時，可將筆刷隨機旋轉 θ 角度，並可在一區間中隨機移動，如方程式(2.1)，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。

$$\begin{bmatrix} P'_{k,s,m,0} \\ P'_{k,s,m,1} \end{bmatrix} = Rot_{2\times 2} \times \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} \begin{bmatrix} P_{k,m,0} \\ P_{k,m,1} \end{bmatrix} + Trans_{2\times 1} \qquad (3.2)$$

$$where \quad m = 1, ..., M$$

3.3 加密方法

完成將影像分層後，不同階層的影像對應不同縮放尺度的密碼圖樣作為繪圖筆刷，以模擬出不同階層影像，由淡畫到濃的加密影像過程如下：

步驟一：從最淡階層 L_0 起，對應全白圖樣的筆刷 P_0，在此階層不論 L_0 的影像內容為何，將畫布 H 填滿白色，其中白為 0，黑為 1；

$$H_i \equiv 0 \tag{3.3}$$

步驟二：接者模擬次淡階層的影像 L_1，以對應最大縮放尺度 s_1 的圖樣 P_1，以該圖樣尺寸的大小將影像 L_1 切割成不重疊的連續區塊 L_{1i}，由判斷每區塊中 L_{1i} 為 1 的數量總合是否大於一定門檻值 t_1，以決定是否在該區塊位置要在畫布上繪製圖樣，而此圖樣是經由方程式(3.2)的幾何轉換結果產生的；

$$\begin{aligned} &if \quad SUM(L_{1i}) > t_1 \\ &H(P'_{k,s,m,o}, P'_{k,s,m,1}) = 1 \end{aligned} \tag{3.4}$$

步驟三：再者模擬影像 L_2，以對應次大縮放尺度 s_2 的圖樣 P_2 之尺寸大小將影像 L_2 切割成不重疊的連續區塊 L_{2i}，由判斷每區塊中 L_{2i} 為 1 的數量總合是否大於一定門檻值 t_2，在此以免混淆先前所放置的密碼圖樣，在繪製的過程中在畫筆刷之前先在欲放置筆刷的位置抹除已存在畫布上的點，再將新畫筆繪製其上；

$$\begin{aligned} &if \quad SUM(L_{2i}) > t_2 \quad then \\ &H_i \equiv 0 \\ &H(P'_{k,s,m,o}, P'_{k,s,m,1}) = 1 \end{aligned} \tag{3.5}$$

步驟四：如同步驟三，以此類推直到完成 L_4 階層影像，得到圖 3.5 最終加密影像。

加密處理的過程中，t_1，t_2，t_3，t_4 的門檻值選擇可隨不同影像調整，才能獲得較佳的影像模擬。而為了避免單一鍵值的密碼圖樣容易被抓出，我們將兩個鍵值的密碼圖樣加在影像之中，在影像產生過程中將兩鍵值的密碼圖樣交替出現，以增加編碼的複雜度，使密碼圖樣不易被破解。

在認證過程中，我們發現基本密碼圖樣的最小縮放尺度所形成的圖樣容易與其他鍵值混淆，因而不具有密碼認證的功能，其明顯的區塊形狀也造成可能被破解的疑慮，且濃度最深的區域常為影像的邊界，是描繪影像最重要的因素，使用隨機圖樣的縮小尺度來拼湊，影像品質甚差，因而在濃度最深的區域影像我們改使用誤差擴散法產生調頻網點，得到較佳的影像品質，如圖 3.6。

圖 3.5 以不同縮放圖樣產生的加密影像

圖 3.6 以調頻網點取代最深階層影像的加密後結果

因誤差擴網與本研究中所形成半色調影像的方式有很大的不同，故先對原始灰階影像進行濃度調整再進行誤差擴散以免使得階調變化太過突兀。由縮放圖樣所能表現的等效灰度約在 235(註)至 255 之間，因而先將灰階影像 0 至 255 作 235 至 255 的線性調整，得到整體影像亮度增加的灰階影像 *I'*，再以 Floyd 與 Steinberg 所提出的誤差擴散法 Floyd-Steinberg Error Diffusion(FSED)[21]產生調頻網點影像。其兩階化如方程式(3.6)所示，設定一固定的臨界值，而將誤差擴散至鄰近未二階化的像素時，需選擇方程式(3.7)之矩陣來分配誤差擴散的比重。

$$h(i,j)\begin{cases}1, & I'(i,j) < Threshold \\ 0, & I'(i,j) \geq Threshold\end{cases} \tag{3.6}$$

$$\frac{1}{16}\begin{bmatrix}0 & 0 & 0 \\ 0 & -16 & 7 \\ 3 & 5 & 1\end{bmatrix} \tag{3.7}$$

得到調頻網點影像 *h* 之後，以及利用不同縮放圖樣之模擬完成 L_0, L_1, L_2, L_3 的加密影像 *H*，以最深階層影像 L_4 作為一遮罩合併兩者，如方程式(3.8)所示，將 L_4 為 1 的部分以調頻網點呈現；L_4 為 0 的部分以不同縮放圖樣拼貼的加密影像呈現，得到最終加密影像 *H'* 如圖 3.6 所示。

$$H' = \left(\left(H \cap \sim L_4\right) \cup \left(h \cap L_4\right)\right) \tag{3.8}$$

(註)最小縮放圖樣尺寸為 25×25，內含 50 個密碼點，其等效灰階的計算為$\left(1-\frac{50}{25\times 25}\right)\times 255 \quad 236$。

3.4 邊界加強

過網的過程本是一種空間解析度的破壞，因而一般在灰階影像轉成二階影像的過網過程前都會先經過影像加強，以加強輪廓使之不致喪失。而本研究不同於一般過網的方式，以有限的階調展現影像，在此影像輪廓必定要明確的勾勒出，才能較接近原來灰階影像。在此以遮色片銳利化(Unsharp masking)增強影像的邊界輪廓[16]，原輸入影像為 *I*，以一低頻濾波器 *b* 將 *f* 模糊化形成 *G* 影像，如方程式(3.9)，再以方程式(3.10)之數學運算得到增強後的影像 *I'*，其中 α 值的範圍在 0 到 1 之間的浮點數，越大則代表邊界加強越明顯；越小則邊界加強越輕微，如圖 3.7 不同參數 α 對最終加密完成的影像有明顯的差異，在本研究在邊界加強中使用 α =0.8。

$$G(x,y) = I(x,y) * b(x,y) = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I(m,n)b(x-m,y-n) \tag{3.9}$$

$$I'(x,y) = \frac{1}{1-\alpha} I(x,y) - \frac{\alpha}{1-\alpha} G(x,y) \tag{3.10}$$

圖 3.7　由左至右 α 值依序為 0.2, 0.5 與 0.8 加強效果下的加密影像

3.5 直方圖等化

影像的直方圖(histogram)代表每個灰度佔整體數量的百分比，可視為一機率密度函數，而直方圖等化(histogram equalization)的目的在延展原來的灰階分布，使得到一灰度分布較均勻的影像，提高整體的對比達到影像增強的目的[16]，尤其對本研究中將原256階調的灰階影像量化分成N階層時，可以保證不同階層影像皆佔有較均等的比例。

$$\Pr(r_j) = \frac{n_j}{n} \tag{3.11}$$

$$\begin{aligned} S_k &= T(r_k) = \sum_{j=0}^{k} \Pr(r_j) = \sum_{j=0}^{k} \frac{n_j}{n} \\ 0 &\le r_k \le 1 \quad and \quad k = 0,1,\ldots,255 \end{aligned} \tag{3.12}$$

$$f(x) = X\min + (X\max - X\min) \times S_k \tag{3.13}$$

首先以方程式(3.11)計算輸入的灰階影像G之(如圖3.8a)直方圖Pr，即灰階j之像素的個數n_j除以總像素數量n所形成的機率函數，如圖3.8c所示。接著以方程式(3.12)計算累加直方圖S_k，如圖3.8e所示。再者以方程式(3.13)，從累加值直方圖計算等化分布的直方圖$f(x)$，使灰階頻率均分布在[Xmin, Xmax]，在此定義Xmin是最小的灰階值(0)，Xmax是最大的灰階值(255)，如圖3.8f所示。將$f(x)$當作映射函數，重先指定每一像素對應的灰階值，最後可得等化後的灰階影像，如圖3.8b所示，其直方圖$\Pr_{eq}$如圖3.8d所示。如圖3.9所示，先經直方圖等化後再作影像分層的處理，分層後的各階層的影像所佔的比例較圖3.4均等，才能保證密碼圖樣在加密後有一定比例的存在。

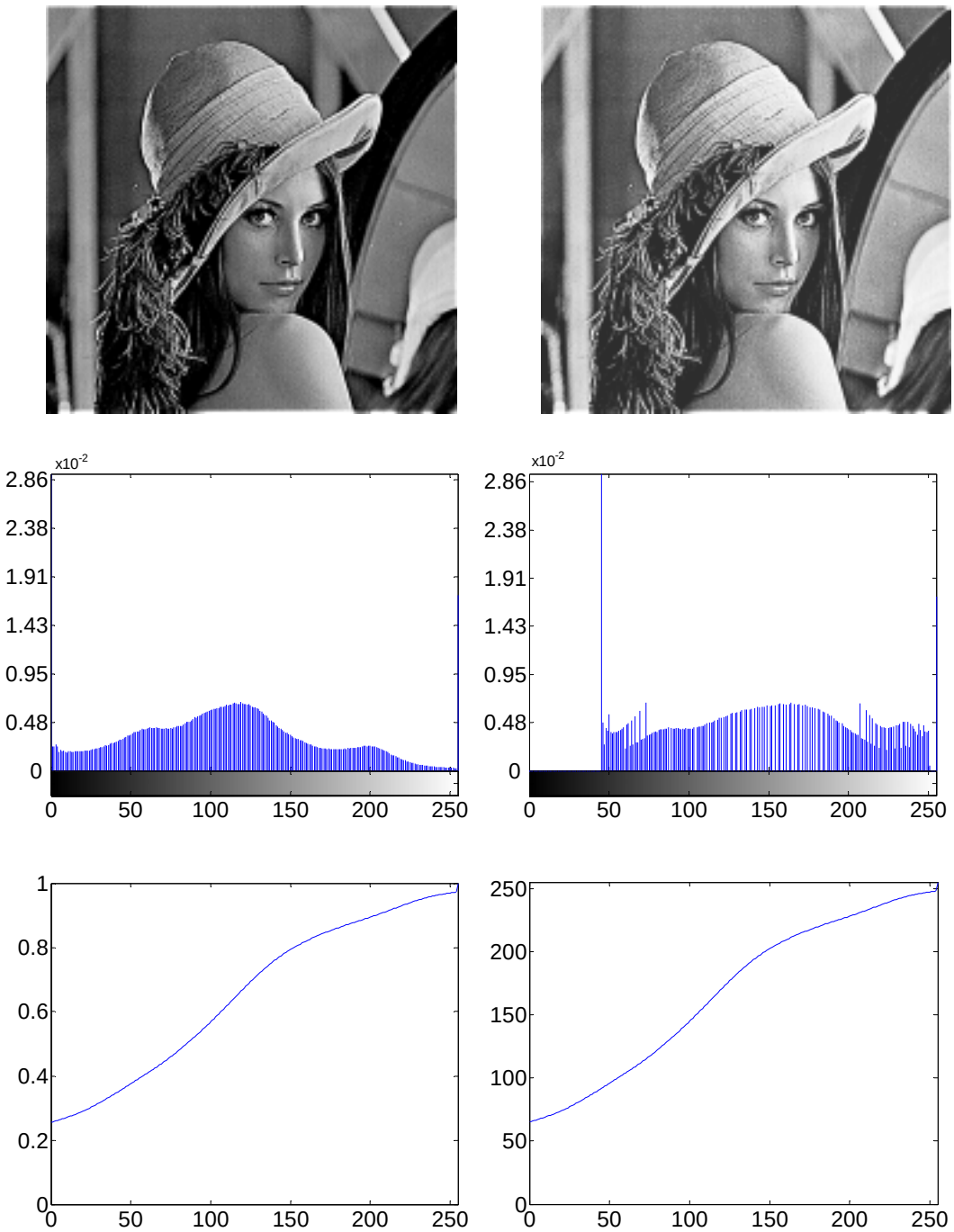

圖 3.8　灰階直方圖等化。(a)輸入的灰階影像 G；(b)輸入的灰階影像 G_{eq}；(c)灰階影像 G 之直方圖 Pr；(d)直方圖等化後的灰階影像 G_{eq} 之直方圖 Pr_{eq}；(e)累加直方圖 Pr 而呈現的單調遞增函數 S_k；(f)以 S_k 計算等化後的灰階分布 $f(x)$

圖 3.9　影像分層由淺至深分別以白、藍、綠、紅、黑代表，經灰階值等化後每階調各佔的比例較圖 3.4 均等

3.6 加密流程

經修正過後的整體加密流程如圖 3.10 所示。在灰階影像輸入之後，以影像增強演算加強影像的輪廓細節與直方圖等化使灰階平均分布；再者將 0 至 255 階的灰階影像等份分成 N 階影像組，每一階層影像皆為二階影像並對應不同縮放尺度的密碼圖樣作模擬行為；由影像階層的淡至濃的順序以不同縮放尺度的圖樣作階調模擬，從最淡階層影像 L_0 起，對應方程式(3.3)，不論 L_0 的內容為何將畫布 H 填滿白色(0)；次淡階層 L_1 對應放大最大的圖樣 P_1，如同方程式(3.4)作該階調的模擬；再者，階層 L_2 對應縮放尺度次大的圖樣 P_2，如同方程式(3.5)作該階調的模擬，在此圖樣繪製於畫布前，先抹除已存有的點再將圖樣繪製其上；以此類推依序完成 L_3 至 L_{N-1}；最深階層影像則將是先產生的調頻網點透過 L_N 遮罩與畫布上的點結合完成最終加密影像。每次選擇圖樣作繪圖的動作時，交替使用兩個鍵值的密碼圖樣，以增加編碼複雜度防止被破解。

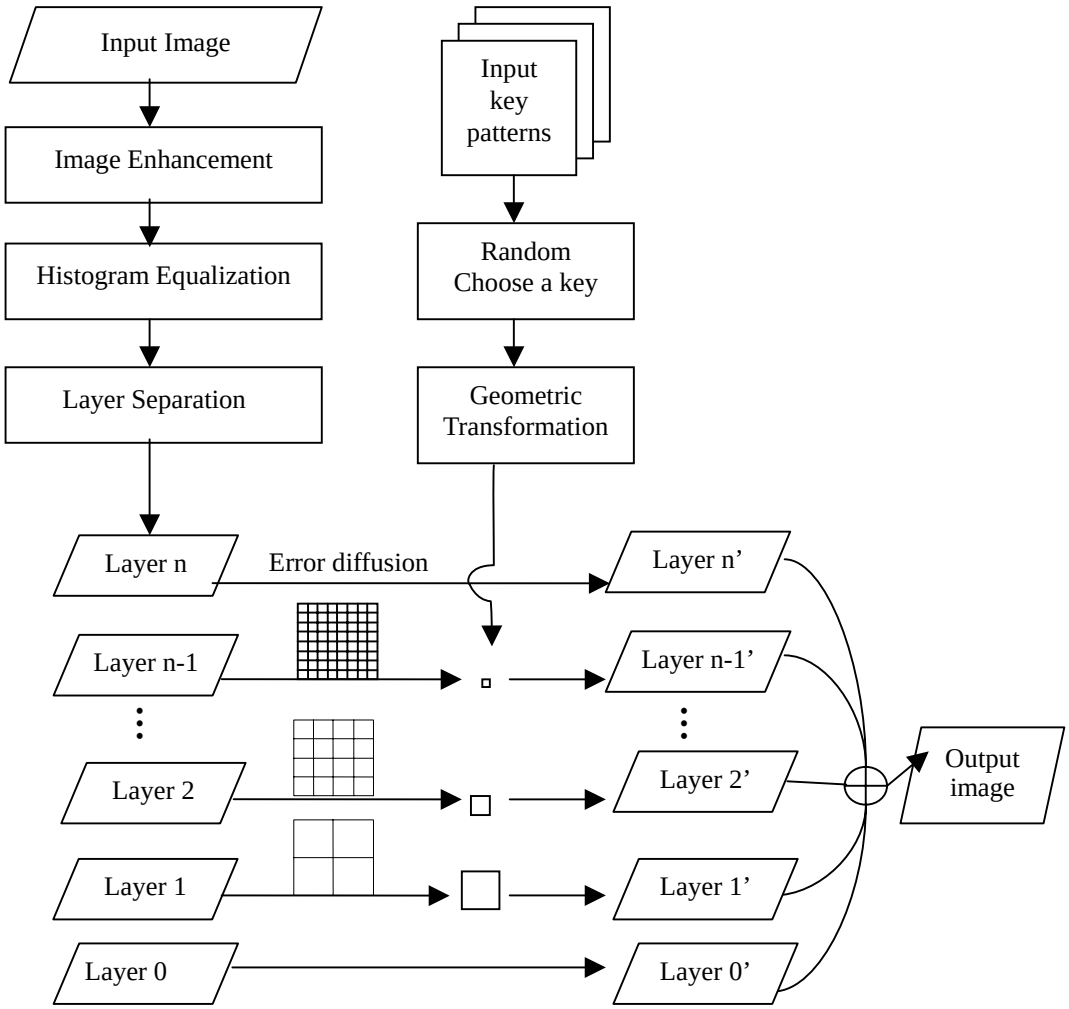
Input Image
Image Enhancement
Histogram Equalization
Layer Separation
Input key patterns
Random Choose a key
Geometric Transformation
Layer n
Error diffusion
Layer n'
Layer n-1
Layer n-1'
Layer 2
Layer 2'
Layer 1
Layer 1'
Layer 0
Layer 0'
Output image

圖 3.10　加密流程圖

3.7 密碼驗證

由於將最深階層取代成調頻網點以後，在最深階層的部分不具有密碼圖樣的存在，因而在密碼驗證應該自動避開該區域。在此以一自動化搜尋適當解碼區域的決策，對該區域進行幾何雜湊法的密碼圖樣之比對。以 480×480 搜尋視窗中的特徵點總數量在 500 到 1000 點之間視為可與 100×100 的密碼圖樣作驗證的適當區域，如圖 3.11 所示框選的區域為可供密碼驗證的區域。在此密碼的驗證事先搜尋適當解碼區域，在該區域中再行幾何雜湊的密碼比對。實驗驗證過程隨機找 10 個適當解碼的候選區域，並在該區域以幾何雜湊隨機選擇 20 次基底進行密碼鍵值的比對，因此一共執行 200 次隨機指定基底的幾何雜湊比對。

圖 3.11　自動搜尋適當解碼的區域