第二章　文獻探討

本章節一開始會先針對本研究所使用到的視覺密碼與離散小波轉換技術做說明，並簡述幾篇關於視覺密碼應用於著作權保護的文章，在這些文章中皆是應用(2,2)-threshold 的視覺密碼方法，且皆以灰階影像為原圖，黑白影像為浮水印來做為實驗的討論對象。

第一節　相關技術介紹

一、視覺密碼

視覺密碼(visual cryptography, VC)技術是由 Naor 與 Shamir 於 1995 年所提出的一種利用視覺解密的加密方法，稱為(*k*,*n*)-threshold 視覺式機密分享機制，最初是設計在黑白影像上，其中 *k* 是還原機密影像時所需份數的最低門檻，*n* 是機密影像被分解的份數。此方法最大的特色是靠人類的視覺系統便能夠對加密影像做解密。當黑白影像在經過加密後會被分解成 *n* 份外觀上只是一張雜亂且無意義的分享影像，這些分享影像會被列印在投影片上，未重疊之前我們並無法得知相關的影像資訊，在將分享影像重疊後，不需要電腦的輔助即可用人眼辨識出黑白影像中的訊息，且這項特色對於解密者來說，本身不需再另外具備密碼學的相關知識，因此提高解密的便利性。

一個(*k*,*n*)-threshold 視覺式秘密分享機制可以表示成兩個 $n \times m$ 矩陣 M_0和 M_1，矩陣 M_0代表白點的分解規則，M_1則代表黑點的分解規則，*m* 代表像素擴展的倍數。公式 2-1 及公式 2-2 即為(2,2)-threshold 視覺式秘密分享機制的矩陣，其中 0

代表白點，1 則代表黑點，當要分解機密影像上的白點時，將陣列 M_0 的欄向量隨機重排，取出第一列的兩個點並填入分享影像 1，第二列的兩個點填入分享影像 2；同樣地，在分解機密影像上的黑點時，將陣列 M_1 的欄向量隨機重排，取出第一列的兩個點並填入分享影像 1，第二列的兩個點填入分享影像 2，當白點與黑點分解完畢後，將分享影像 1 及分享影像 2 重疊在一起後即產生一張重疊影像。表 2-1 則為(2,2)-threshold 視覺式秘密分享的圖示，從表 2-1 可看出機密影像上的一個點在重疊影像上會擴展為兩個點，因此，在利用視覺密碼對影像加密時，重疊影像會被擴展為機密影像的 2 倍(侯永昌，杜淑芬，2004)。

$$M_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \tag{2-1}$$

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2-2}$$

表 2-1　(2,2)-threshold 視覺密碼分享及重疊之結果

機密影像上的像素	分享影像 1	分享影像 2	重疊影像
□	◧	◧	◧
	◨	◨	◨
■	◧	◨	■
	◨	◧	■

一般而言，(k,n)-threshold 視覺式秘密分享機制必須滿足下列三項條件(Naor and Shamir, 1995)：

(一)對於任何一個屬於白點的 M_0 矩陣，任取其中 k 列經過"OR"運算所產生的 m 維向量 V 必須滿足 $H(V) \le d - \alpha m$。

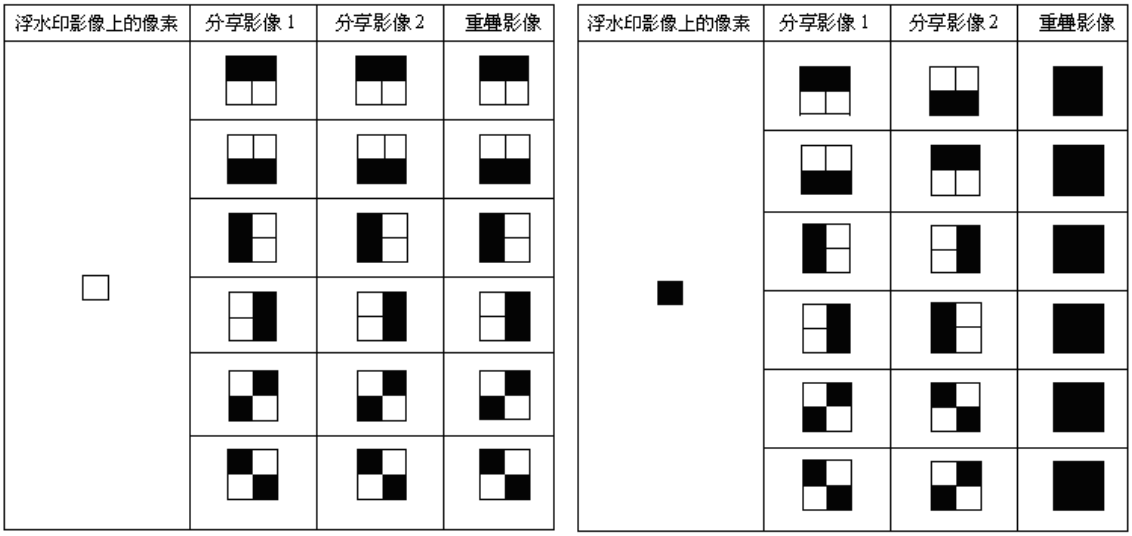
(二)對於任何一個屬於黑點的 M_1 矩陣，任取其中 k 列經過"OR"運算所產生的 m 維向量 V 必須滿足 $H(V) \ge d$。

(三)假設 D_0 與 D_1 分別代表由 M_0 與 M_1 中任取其中 q 列($q < k$)所形成的 $q \times m$ 子矩陣，將 D_0 與 D_1 做行向量隨機重排，所有可能的結果形成的兩個矩陣集合是無法分辨的。

其中，d 表示一個門檻值，m 代表像素擴展的倍數，α 表示分享影像中黑點與白點的相對差值。在上述三項條件中，前二項條件為對比條件，表示大於等於 k 份以上的重疊影像上的黑色區域與白色區域應該有 $\alpha \cdot m$ 的對比，第三項為安全條件，表示 k 份以下的重疊影像，是無法分辨黑色與白色的差異，亦無法從中分析出與機密影像有關的資訊。

由於重疊影像在擴展為原機密影像的 2 倍時會產生影像變形的問題，因此，基於浮水印影像明確性的條件，本研究所採用的分享規則如表 2-2 所示。在分解黑白影像時，影像上的每一個點會被放大成原來的 2×2 倍以解決重疊影像變形的問題，且黑點與白點分別有 6 種加密規則，每種規則被使用到的機率為 1／6。分享影像在重疊後，白點會被還原成 2 個黑點及 2 個白點的 2×2 區塊，如表 2-2 (a)所示；黑點則被還原成全黑的 2×2 區塊，如表 2-2 (b)所示。由於人眼並無法分辨像素與像素之間的差異，而是將多個像素合在一起平均看待，因此由白點與黑點的重疊影像之間的對比，人眼便可在重疊影像上區分出黑色與白色的差異。

表 2-2　(2,2)-threshold 視覺密碼分享規則



(a)　　(b)

二、離散小波轉換

(一)頻率域

在影像處理的技術上大致上分為兩類：空間域(spatial domain)與頻率域(frequency domain)(張真誠，黃國峰，陳同孝，2003；連國珍，1999；繆紹綱，1999)，本文所使用的技術屬於頻率域這一類。頻率域與空間域最大的不同就是頻率域能夠透過轉換公式將影像從空間域轉為頻率域，再依影像中頻率的不同分成低頻帶和高頻帶，低頻帶像素與像素之間的變化較少，影像較平滑，圖 2-1 是一張灰階影像，其中 A 部份就是所謂的低頻帶，由於變化較少，因此只要稍做更動很容易就被人眼所察覺，屬於影像中重要的區域；高頻帶則是像素與像素之間的變化較多，影像較複雜，如圖 2-1 的 B 部分就是所謂的高頻帶，由於變化較多，因此在修改像素值時，較不容易被人眼所察覺，屬於影像中不重要的區域。一般在做影像壓縮也是利

用高頻帶較不重要的特性，將之做刪除或修改的動作，以減少儲存量。由此可知，在將浮水印嵌入到影像中時，高頻帶應為較佳的藏密位置。

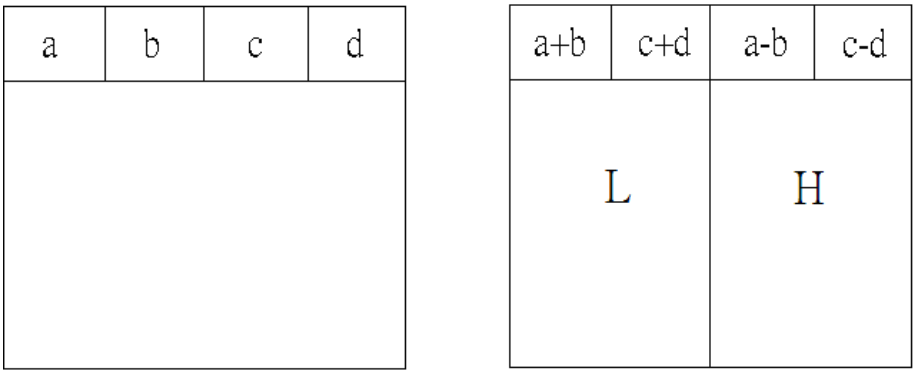
圖 2-1　灰階影像

(二)Haar 轉換

目前在學術界，關於離散小波轉換的模型有很多種，例如：Antonini、HAAR、Daub4、villa4 等(王旭正，柯宏叡，2003)。本文所採用的數學模型為一階 Haar 轉換(張真誠，黃國峰，陳同孝，2003；連國珍，1999；繆紹綱，1999)，包含水平小波轉換與垂直小波轉換，是屬於較簡單的作法。

水平小波轉換的作法是將灰階的原始影像取出第一列的第一個像素 a 的值與第二個像素 b 的值，如圖 2-2 (a)，將 $a+b$ 的結果放入圖 2-2 (b)的 L 部分，也就是所謂的低頻部分；將 $a-b$ 的結果放入圖 2-2 (b)的 H 部分，也就是所謂的高頻部分，以此類推，第三與第四個像素，第五與第六個像素...，當第一列的像素處理完畢時，接著取出第二列的第一與第二個像素，第三與第四個像素...等，

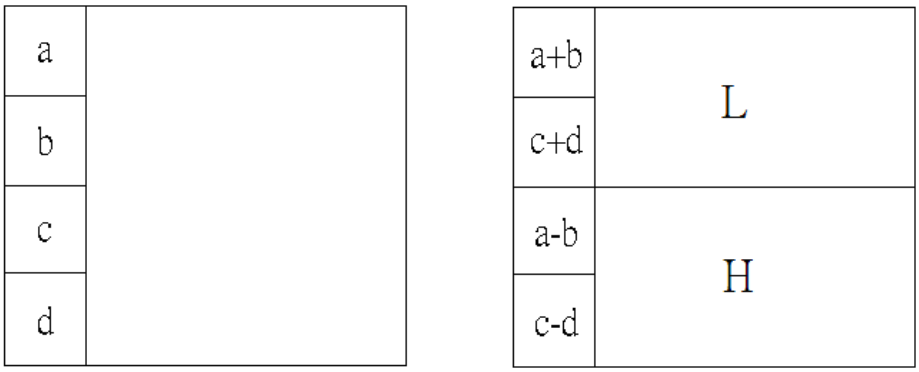
直到整張影像處理完成。



(a) (b)

圖 2-2　水平小波轉換

同理，垂直小波轉換的作法是將原始影像取出第一行的第一個像素 a 的值與第二個像素 b 的值，如圖 2-3 (a)，將 $a+b$ 的結果放入圖 2-3 (b)的 L 部分，也就是所謂的低頻部份；將 $a-b$ 的結果放入圖 2-3 (b)的 H 部份，也就是所謂的高頻部份，以此類推。



(a) (b)

圖 2-3　垂直小波轉換

最後，原始影像轉換後的頻帶分佈如圖 2-4 所示。在

一張影像中，物體邊緣的部份由於差值較大，所以即便是受到更動也不容易被人眼所查覺，反之，物體平滑的部份由於差值較小，所以只要稍有更動就可能被人眼所查覺。換句話說，差值越小的部份也就是越低頻的部份就越重要，在圖 2-4 中 LL 為影像中最重要的部份，而 HH 則為人類視覺較不易察覺的部份，因此在將浮水印影像藏入原始影像時，HL、LH 及 HH 會是較佳的隱藏地點。圖 2-5 為將圖 2-1 經一階離散小波轉換實作後的影像。

LL	HL
LH	HH

圖 2-4　一階離散小波轉換

(a) 水平小波轉換　　(b) 垂直小波轉換　　(c) 小波轉換完成

圖 2-5　一階離散小波轉換實作

在小波轉換轉回的過程中，以垂直小波轉換為例，如圖 2-6 (a)，首先取出小波影像中 L 頻帶第一行的第一個像

素 $a+b$ 的值與 H 頻帶第一行的第一個像素 $a-b$ 的值，將 $a+b$ 和 $a-b$ 相加再除以 2 的結果即可還原原始影像的第一行第一個像素值 a，而將 $a+b$ 和 $a-b$ 相減再除以 2 的結果即可還原原始影像的第一行第二個像素值 b，如圖 2-6 (b)，以此類推，即可還原整張原始影像。

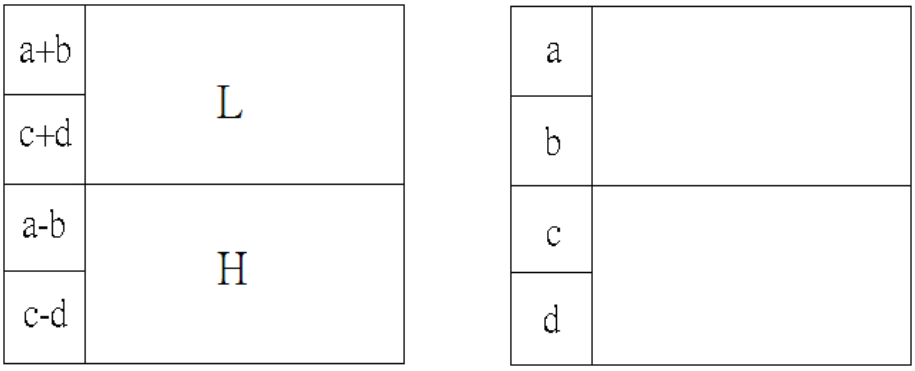


圖 2-6　垂直小波轉換轉回

第二節　　相關文獻介紹

一、侯永昌與沈昌興及 Hwang 所提之方法

由於侯永昌與沈昌興(2000)認為影像經過數位訊號處理後，其最高位元較其他位元有較低之變動率，因此，他們先取出原始影像的最高位元後，存入 BitPlane0，再將 BitPlane0 經過虛擬隨機重排產生 BitPlane0’，依每像素擴展為原來的一倍的方式，將 BitPlane0’像素值為 0 的像素轉換為“01”及像素值為 1 的轉換為“10”，來產生第一份分享影像為 share1，並將 share1 與浮水印依據(2,2)-threshold 視覺密碼機制來產生 share2，當浮水印之像素值為“0”，若 share1 為“01”則相對之 share2 亦為

“01”，若 share1 為“10”則相對之 share2 亦為“10”；當浮水印之像素值為“1”，若 share1 為“01”則相對之 share2 為“10”，若 share1 為“10”則相對之 share2 為“01”。當要驗證所有權時只需取出疑似盜版影像中的 share1 與所有者手中的 share2 重疊，即可產生浮水印。

Hwang (2000)在“A Digital Image Copyright Protection Scheme based on Visual Cryptography”所提出的是結合視覺密碼與空間域技術的方法，首先利用 key 值隨機從原圖中取出一組像素的集合，根據集合中像素的最高位元與浮水印的像素來依視覺密碼的原理產生驗證資訊。當要取出浮水印來驗證所有權時，從需要被驗證的影像中，利用 key 值取出一組像素的集合，根據集合中像素的最高位元與驗證資訊來做 OR 運算並產生浮水印以驗證所有權。此法在驗證所有權的過程中，除了會產生不同的兩張影像有可能最高位元是相似的情形之外，在使用視覺密碼技術時，此法並沒有滿足視覺密碼安全性的條件。

侯永昌與沈昌興(2000)以及 Hwang (2000)所提出的方法相當類似，皆是利用空間域的理論，來針對影像中的最高位元做浮水印的藏入，雖然不需修改原圖就能夠藏入浮水印，但是若像素值為 127 或 128 也就是二進位為 01111111 或 10000000 的情況時，最高位元平面很容易在遭受到攻擊時，由白點轉為黑點或黑點轉為白點，造成判斷上的錯誤，且相較於頻率域的方法，空間域的強韌性會顯得較弱。此外，侯永昌與沈昌興以及 Hwang 的作法會使得分解影像 share2 不具有視覺密碼的安全性，而且其未將浮水印藏入影像中，在判斷所有權時很容易產生因特徵值相似而誤認的問題。

二、Chen and Hou 所提之方法

Chen and Hou (2001)在“Yet Another Asymmetric Digital Watermarking based on a Visual Cryptographic Approach”這篇論文中，所提出的方法是先利用(2,2)-threshold 的視覺密碼理論將浮水印分解成二份分享影像，分別為 share1 及 share2，將原始影像利用 key 值打亂後產生一張隨機重排過的原始影像後，第一步先從浮水印與 share1 中取出相對應的像素，依判斷條件來修改重排過的原始影像的像素，藉由修改原始影像的像素依序將浮水印藏入重排過的原始影像中，修改完後將原始影像利用 key 值回復為未打亂前的影像，即產生一張 stego-image。

第二步再根據從浮水印與 share2 中取出相對應的像素，依判斷條件來修改 share2 的像素，依序修改完後產生 share2’，修改後的 share2’則成為取出浮水印的 key 值。當要驗證所有權時，只需利用 key 值將被驗證影像打亂之後，再將打亂的被驗證影像與 share2’重疊，即可產生浮水印影像。雖然此法在藏入及驗證浮水印時有簡單快速的優點，但是被浮水印影像在經過一些影像攻擊後，經過人眼辨識的結果，取出的浮水印並不是非常的清楚，因此 Chen and Hou (2001)提出的方法並沒有達到強韌性的要求。

三、Hou and Chen 所提之方法

Hou and Chen (2000) 在“An Asymmetric Watermarking Scheme based on Visual Cryptography”所提出的方法是先將 Naor 與 Shamir 提出的視覺密碼原理略做修改，在 share1 黑色像素的部份是改用灰階值等於 247 的像素來取代，如圖 2-7 所示，利用圖 2-7 將浮水印分解成二份分享影像為 share1 及 share2，藉由修改原始影像的像素來將 share1 藏入到原始影像中，當要驗

證所有權時，只需將 share2 與被浮水印影像重疊即可產生浮水印。

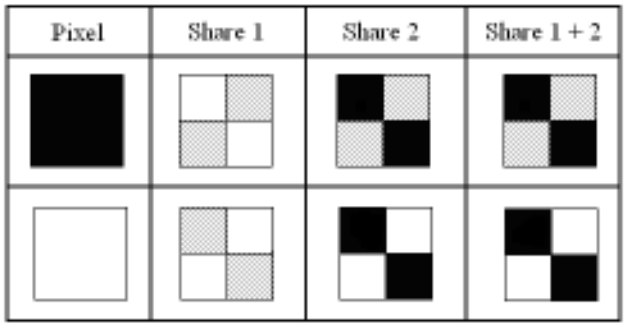


圖 2-7　Hou and Chen 所提之(2,2)-threshold 視覺密碼概念

此法與 Chen and Hou (2001)所使用的方法相當類似，其最大的不同點在於此法在將 share1 藏入到原始影像前並未先將原始影像做打亂的步驟，且此法在藏入浮水印時只針對原始影像進行修改，在程序上較 Chen and Hou 所提的方法更為簡單。其最大的缺點是在於強韌性不足及在驗證所有權時需要原圖的輔助(Chang and Chuang, 2002; Hsu and Hou, 2005)。

四、Hsu and Hou 所提之方法

Hsu and Hou (2005)在“Copyright Protection Scheme for Digital Images using Visual Cryptography and Sampling Methods”所提出的方法則是利用統計學中的樣本平均抽樣分配(sample distribution of means, SDM)來加強在使用視覺密碼規則的安全性及強韌性。其藏入浮水印流程圖如 2-8 所示，首先利用虛擬隨機亂數產生器從原始影像中隨機抽取出一組像素，像素個數必須要大於或等於 30 以滿足中央極限定理，再計算每組像素的平均值後，依據判斷條件及視覺密碼的規則來產生主控影像 M，最後再根據視覺密碼的加密規則產生所有權影像 O，便完成隱藏

浮水印的動作，所有權影像為原始影像所有者持有，以便將來驗證所有權之用。

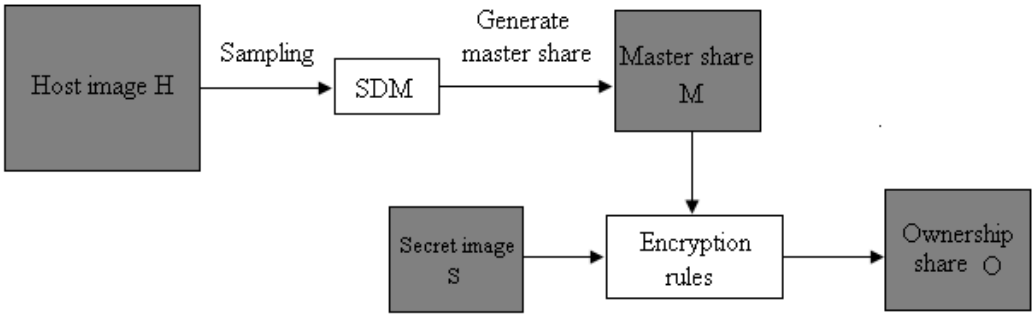


圖 2-8　Hsu and Hou 所提之隱藏浮水印流程圖

圖 2-9 為驗證所有權流程圖，當要驗證所有權時，先根據先前取出主控影像的方法取出 M’，再將影像所有者手中的所有權影像 O 與 M’利用視覺密碼的解密規則來產生浮水印影像。

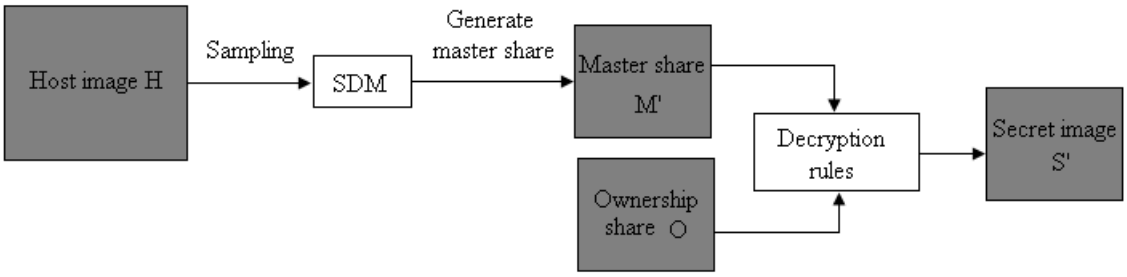


圖 2-9　Hsu and Hou 所提之驗證所有權流程圖

雖然 Hsu and Hou (2005)利用常態分配來加強藏入浮水印的安全性，但是在隱藏一個浮水印像素時，此法需要較多原始影像的像素來做輔助，且未將浮水印藏入到影像中可能會產生誤認所有權的問題，因此在將浮水印藏入原始影像後，則需要再透過具公信力的第三者認證來保障智慧財產權。

五、Lou, Tso, and Liu 所提之方法

Lou, Tso, and Liu (2007)在“A Copyright Protection Scheme for Digital Images using Visual Cryptography Technique”所提出的方法是先將原始影像做三階的離散小波轉換，如圖 2-10 所示，根據中頻帶與低頻帶相對位置的像素來求出特徵值，再利用特徵值及其位置依據所設計之密碼簿來產生秘密影像，密碼簿如圖 2-11 所示，若求出之特徵值為 0 則再計算此特徵值所在位置之總和除以 4 之餘數，利用特徵值與餘數來依照密碼簿的規則及浮水印的像素去判斷秘密影像的像素，反之，若特徵值為 1 也是採用相同的做法來判斷秘密影像的像素，依序判斷完所有的浮水印及特徵值後即可產生一張秘密影像 S，之後再將秘密影像 S 交由具有公信力的認證中心做記錄，以便將來驗證所有權之用。

當要驗證所有權時，先將需要被認證的影像利用先前的方法取出一張公開影像 P 後，再將秘密影像 S 與公開影像 P 經由 XOR 運算後，即可產生所藏入浮水印影像。此法在藏入浮水印及驗證所有權的過程中，所使用的密碼簿只是類似視覺密碼的一種方法，並非題目所提及的視覺密碼技術，其原因為視覺密碼原先在設計的時候是將分享影像設計在投影片上，所以在重疊 2 張分享影像時所採用的運算應該是 OR 運算而不是 Lou 等人(2007)所使用的 XOR 運算。因此，關於此法所使用技術的這個部份是需要再進一步去討論的，而此法在求出特徵值所使用的方法則是類似前一節所提到統計學上的概念，利用常態分配的特性來加強浮水印的安全性，避免被攻擊者猜出所藏入浮水印的規則。

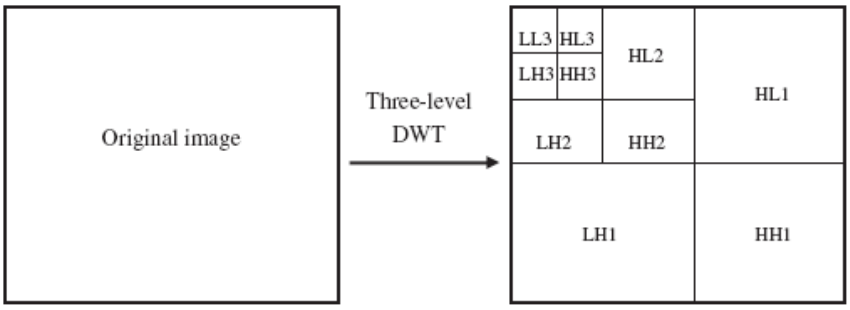


圖 2-10　三階離散小波轉換的實作圖

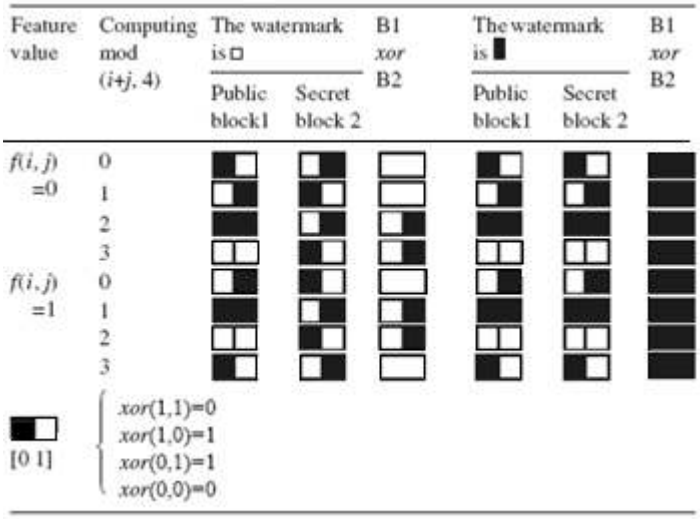


圖 2-11　Lou 等人所提出之密碼簿

六、Chang and Chuang 所提之方法

Chang and Chuang (2002)在“An Image Intellectual Property Protection Scheme for Gray-Level Images using Visual Secret Sharing Strategy”所提出的方法同樣也是採用視覺密碼與空間域技術，一開始先從被打亂的原圖中取出一張子圖，依據子圖來產生第一份分享影像為 share1，而第二份分享影像則利用一張與浮水印大小相同的影像及應用 Hwang and Chang (2001)所提出改良後的視覺密碼方法來產生為 share2，再依浮水印的像素來修改 share2 的像素，使得 share1 與 share2

重疊後會與浮水印相同，修改完後的 share2 則會交由所有者持有。在驗證所有權時，只要依照之前的方法從被驗證影像中取出 share1，再與所有者手中的 share2 重疊後即能夠顯示出浮水印來驗證所有權。此法在藏入浮水印時，除了需要原圖與浮水印之外，還需要一張和浮水印大小相同的影像來產生 share1 以協助浮水印的藏入。由於此法未藏入浮水印到影像中，因此在驗證所有權時，很可能會因為被驗證影像和原圖太相似而產生誤解的問題。

七、Chang and Wu 所提之方法

Chang and Wu (2001)在“A Copyright Protection Scheme of Images based on Visual Cryptography”所提出的方法是先將原始影像打亂後，再將打亂後的影像切割成數塊區塊，每一個區塊由數個像素所組成。計算每塊區塊內像素的平均值後，再將影像做第二次的切割，使其中的每塊區塊包含 4 個平均值，根據平均值的大小轉換成黑點與白點後，依視覺密碼的方法與浮水印做比較，最後會產生一份 share 來當作驗證所有權時所需的金鑰。此法利用空間域技術來取出原始影像的特徵值，藉由特徵值與視覺密碼來隱藏浮水印，其最大的缺點就是會產生誤認所有權的問題。