第一章、緒論

1.1 前言

安全文件係指有價值性或是具有證明能力的文件，包含有價證券與證件，例如：鈔票、股票權狀、身分證、護照等，因其代表的價值與法律效力使得安全文件需要特殊的設計以防止遭不肖人士的偽造或變造。近年資訊科技、網路與影像相關設備，技術愈精進、價格日趨便宜，使知識的大量複製與傳遞成為可能，只需合理花費的價格就可獲得高品質的複製品，資訊科技固然便利了使用者，但也容易遭受不當的使用，因而數位版權管理的機制(Digital Right Management)日趨重要[12]。自從攝影技術發明後，安全文件的安全性就受到衝擊；當今掃描器、印表機、影印機等圖文複製器材發展越進步、價格愈低廉，無須受訓練的技術，即可獲得高品質的印刷品，而安全文件也需要提高技術困難性與品質解析度以抵抗目前最大的威脅。

目前安全文件的防偽趨勢是主要利用材料與印製方式的特性朝光學可變(Optical Variable Devices, OVD)的圖像防偽技術發展[17][18]，不但在使用上也可輕易地辨別，而且現在的圖文複製設備無法呈現這種特殊的光影變化，因此各國鈔券無不加此道防偽特徵，例如：不同視角觀察呈現不同色彩的變色油墨、旋轉時有如彩虹般顏色變化的全像片等。近年利用數位影像處理技術調整影像內容產生具有防偽功能的安全文件也日益興起[1][6][10][11][14][24]，除了文件製作成本上有市場競爭性外，透過數位印刷生成每張不同的文件內容，突顯加密的獨特與唯一性更能有效的保護文件安全。

為了防止不肖人士非經授權的複製、偽造或變造重要文件，而在文件中加入秘密資訊以提供作認證(identification)、說明(annotation)或授權使用(copyright)的功能，即稱為資料隱藏技術，其應用於數位檔案的研究已有多項發表，也已有商品化的應用，但希望影像在印列輸出後還能保有浮水印訊息，則必須考量輸出設備的限制與特性。印刷文件藏密的困難在於三點[6][22][24]：1、因輸出設備階調的限制，輸出灰階影像之前會先經過半色調處理形成兩階影像，以提供印製設備作著墨或不著墨的決策，因此在半色調處理程序所造成的階調變化，或者兩階影像本身相對於連續調影像在藏密方面的限制都是需要考量的因素；2、印刷品是由油墨與紙張的物理與化學交互影響下產生，而其中最顯著的變化就是網點擴張效應，會使得鄰近網點相互混合而不易分辨；3、印刷品是實體影像必須以額外的設備取得其中的資訊作解碼或驗證，而在取樣差異的影響下，可被完全重建的資訊有限。

為了解決上述問題，相關領域的學者提出一些解決方案，但仍存在著一些問題，譬如針對第一點印刷圖像是以兩階調呈現的限制方面，部分研究利用半色調後的兩階影像為基礎，透過調整網點大小、移動網點位置、或是以反半色調處理(inverse halftoning)模擬輸出影像實際所呈現的效果，再利用調整原灰階影像的亮暗或調整頻率域係數的方式達到藏密目的，往往為了維持影像品質與密碼隱密性的考量，選擇在人眼較不易察覺的位置作加密，也因如此可藏密的數量與位置受到影像內容的限制；其中也有不考量半色調處理程序的加密研究，大致上的概念是將半色調以及掃描與印列過程視為訊號通道上的干擾或是頻率域上的攻擊來作設計[9][22]，本研究以討論二階影像加密為主，此類型研究則不列入討論。第二點避免網點擴張效應對密碼的破壞方面，由於此因素是數位的兩階影像在印列輸出成文件後能否保留密碼資訊的關鍵，部分研究以限制影像解晰度方式來達到目的，但如此與一般使用印刷品的習慣相牴觸，且

加密後產生的變動也比較容易被識破。第三點在解碼程序上，大部分研究都使用掃描的方式萃取影像特徵，再予以解密，而往往需要一些額外的資訊輔助影像定位，若影像經過裁切後喪失了邊界資訊就無法正確解碼，另外，當應用於大型影像解密時或者是改以非接觸式的取像方式取代掃描器(例如攝影機搭配適當的顯微鏡頭)，針對解析度足夠的部分影像進行解碼的動作，以加速驗證的效率，在這樣的前提下，加密技術的本身就要可以抵抗裁切與幾何變換。

為解決先前研究的諸多限制，我們欲提出一種以網點為基礎的創新影像加密方法，使之可實際因應印列輸出作為底紋影像之應用。希望可以解決以下問題：

1、產生半色調的加密影像作為輸出之應用

2、減輕網點擴張對印列輸出的影像的影響

3、可針對裁切後的局部影像作解碼或認證的動作

1.2 文獻探討

由於半色調過程是影像印列輸出必經的處理之一，故在此介紹數位網點的種類與特性，並探討考量半色調處理過程之數位浮水印技術相關研究的優缺點比較。

1.2.1 數位網點的種類與特性

半色調是印列輸出過程其中之一的處理步驟[21]，由於輸出設備只能控制著墨的有無，不能直接控制墨的濃淡，因而灰階影像在印列之前必須轉成二階影像，半色調即是一種利用調整網點的大小與排列方式以模擬連續階調影像的方法，由此印列輸出之二階影像透過人眼在一定距離的觀察，即類似通過一高斯低頻濾波器對鄰近的點作積分而重建灰階影像。網點圖樣的型式可分集中式與分散式的網點，前者點大小不一，後者點大小一致；而其圖樣排列方式有規律與不規律出現，透過調整不同的網點型式與排列方式可以產生不同的網點影像。其中最常見於商業印刷的網點型式為規律出現的集中式網點(clustered and periodic-dot pattern)，亦可稱為調幅網點(Amplitude Modulation, AM)，產生不同大小規律出現的網點模擬灰階效果，點陣調色法是最常見的演算方式，先將影像劃分成不重疊的連續區塊再以臨界值矩陣(如表 1.1)針對影像區塊一一作半色調處理，最終可得調幅影像，如圖 1.1(a)所示；另一常見的分散網點的隨機出現(Dispersed and stochastic-dot pattern)，亦稱調頻網點(Frequency Modulation, FM)，必須透過數位化的方式產生大小一致的網點利用排列的疏密模擬出灰階效果，如圖 1.1(b)所示，目前的噴墨印表機多使用此種網點生成高解析晰度的文件。

35	49	41	33	30	16	24	32
43	59	57	54	22	6	8	11
51	63	62	46	14	2	3	19
39	47	55	38	26	18	10	27
29	15	23	31	36	50	42	34
21	5	7	12	44	60	58	53
13	1	4	20	52	64	61	45
25	17	9	28	40	48	56	37

表 1.1 點陣調色法中的臨界值矩陣

(a)

(b)

圖 1.1 不同型式網點構成之半色調影像。(a)調幅網點; (b)調頻網點

半色調影像不限於以調幅或調頻網點產生[19]，調幅網點雖然在單一圖樣上表現的很粗糙，但其規律排列的特性，反而降低人眼對細部缺陷的敏感度；細部觀察隨機出現的網點，其雜亂無法呈現規律的特性非常適合用於藏密，且其生成影像的過程中加入的隨機參數也會使得每次產生的隨機網點影像排列的位置有所不同，使影像具有獨特性，並增加了偽造的複雜度。

1.2.2 資料隱藏

在文件、影像、聲音與影片等檔案中加入額外訊息，即為資料隱藏技術(information hiding)，又因應用目的的不同大致可再細分為數位浮水印(watermarking)、偽裝術(steganography)與密碼學(Cryptography)[15]。數位浮水印主要以宣告著作權為主，辨識文件的真偽與出處等，其中也包括藏入序號作為版本或身分的確認；偽裝術是一種科學兼藝術的方法，加密後的訊息任何人都可以取得，但只有接收訊息的一方知道藏密的位置，可解譯出傳送者真正想要傳達的訊息，譬如中國古代秘密書信的往來，當接收者收到來自傳送者的文件，再罩一層只顯示加密位置的遮罩片，即可呈現秘密訊息；而密碼學與偽裝術有些不同，密碼訊息必須透過一特定的轉換方程式才會呈現，偽裝術主要想保護的是轉換的方法，而密碼學主要保護傳送的訊息，這是兩者最大的不同。以上這三類技術皆有強健性與易碎性的方法供不同目的的使用，強健性者強調密碼在經過可能的攻擊情況下還能保留下來，譬如在相片影像中藏入拍攝日期，即使相片經過修改或時間變遷產生了變化，還是可以找出原加入的訊息供證明之用途；而易碎性者在經過攻擊後密碼不存在，反應出文件是否經過處理，譬如將易碎性的資料隱藏在公文之中，可證明公文是否經過竄改的。另外以藏入訊息的種類區分，當加密訊息是圖形目視浮水印時，解碼後常常必須要以人眼輔助作密碼判別；而當解密後的訊息為數字、文字或隨機密碼者，則有利於以機器作判讀，達到全自動化的優勢。

本研究中創新的資料隱藏方法屬於數位浮水印技術，以作為文件真偽判斷與序號認證為目的，將隨機點分布的圖樣藏入半色調影像中，搭配機器閱讀的方式，達成全自動的認證系統。

1.2.3 半色調影像加密研究

Walter Bender等人在1996年提出利用擬似隨機(Pseudo-random)的方式指定加密的位置[1]，以此將密碼分散於影像中，並些微地調整區塊影像灰階的亮暗程度作為加密處理，而加密後的數位影像經過印列與掃描回數位檔案模式後，仍可以統計學的方式作密碼的驗證。此加密方法可在印列與掃描的處理程序後保留密碼資訊，是數位浮水印應用於實際印列輸出的一大突破。但還是必須考量不同輸出狀態下的變因並作適當的參數調整，且必須以額外資訊作影像定位的處理，成為實際應用的一大限制。

Ming Sun Fu 與 Oscar C. Au 在 2000 年提出同樣以擬似隨機方法指定加密的位置[2]，但加密的對象改為二階影像，藉由調整像素點的 0(白)與 1(黑)作為加密處理，並且為了降低加密後對影像品質的破壞，選擇在密碼位置的鄰近像素中選擇一改變後對影像品質較無影響之像素作補償，以維持加密前後區域濃度的一致性；2002 年再提出 MDHED(Modified Data Hiding Error Diffusion) [3]，同樣將密碼藏在事先指定的位置上，以改進先前研究的影像品質為目的，從有原始灰階影像的情況下，在半色調的過程中對加密位置不作半色調處理，但將其與其他非密碼位置在過網後產生的誤差擴散至鄰近未過網區域的像素。這兩種加密方式只在影像品質方面有所差異，而因其皆不考量影像內容決定加密位置，導致加密影像輸出後在某些區域可能因為網點擴張而漏失資訊，輸出後尤其白點容易被周圍的黑點所掩蓋，而解碼前也必須以定位資訊校正數位影像。

Hagit Zabrodsky Hel-Or 在 2001 年提出以點陣調色法為基礎，帶入兩個不同的臨界值矩陣作為密碼訊息[8]，由於設定的兩個臨界值矩陣皆可產生分散式的網點，加密完成的半色調影像也呈現分散式網點的特性，而無法重外觀上察覺半色調影像加密與否的差異性。

此研究中原輸入影像的灰度必須在某一範圍內，才能具體呈現不同臨界值矩陣之間的差異，因此不適合對太濃與太淡的影像加密；在解碼前也必須將影像座標作精確的校正，才能正確解密。

Yu-Chee Tseng 在 2002 年提出利用二階秘密矩陣 K 與一比重矩陣 W 以密碼學的觀點達到二階影像作藏密的目的[20]。首先將原輸入的二階影像 F 劃分成不重疊的連續區塊，加密後的二階影像要維持以下的數學運算關係，

$$SUM\left(\left(F_i \oplus K\right)\otimes W\right) \equiv b_1 b_2 ... b_r \bmod 2^r \tag{1.1}$$

其中⊕代表點對點分別執行 OR 運算，⊗則是代表對每一區塊中的數值作點對點的相乘，SUM 是將運算完成後矩陣內的數值作一累計運算，而只需對原輸入影像 F 的每一區塊矩陣至多作兩位元的變動，即可完成加密影像 F'，藏入的訊息是 $SUM\left(\left(F_i^{'} \oplus K\right)\otimes W\right)\bmod 2^r$。此方法的優勢在只須對原二階影像作些微的變動即可嵌入大量的訊息，改變了二階影像藏密容量之限制。然而該研究對於實際印列輸出影像仍有諸多限制，例如網點擴張導致點不易分辨，以及面臨幾何攻擊時的影像定位。

Ming Sun Fu 與 Oscar C. Au 在 2004 年也提出一個以密碼學為基礎的網點加密方法[4]，與 Tseng 的方法有很大的差異在於採用重疊的方式將原二階影像 F 劃分成連續區塊，也由於這樣的變動使得加密後可針對局部影像作解碼，抵抗裁切攻擊。以一自訂尺寸的二階秘密矩陣 K，與原二階影像的區塊影像 F_i 作 OR 運算，並視其結果的總合為奇數(代表 1)或偶數(代表 0)，

$$SUM\left(F_i \oplus K\right) \equiv \bmod 2 \tag{1.2}$$

加密後影像之運算結果應與欲藏入的二階密碼圖樣有對應關係。該研究的特色在於將加密演算寫在灰階影像半色調的過程中，以加密後產生的半色調誤差值是否超過一定的門檻值，再決定應不應該做加密的變動，每個像素點的半色調處理過程包括先產生二階影像，

再計算方程式(1.2)為奇數(1)或偶數(0)對應密碼影像得到該不該作變動，以及變動後的半色調誤差是否在不影響影像品質容忍範圍之內，作為加密的決策。雖此加密方式相對於[3]可獲得更好的影像品質，並且可針對局部影像解密；但其最大的限制在印列輸出後的網點擴張影響，以及影像定位問題，且只適合加入圖形目視浮水印，實際應用方面只限於數位檔案。

Kacker與Allebach在考慮輸出條件下在頻率域加密的方法，對原灰階影像劃分連續區塊並作離散餘弦轉換(DCT)，以調整係數值的方式作加密處理，再以DBS(direct binary search)的方式尋找輸出前後影像品質影響最小的適當位置放置網點[10]。採用旋轉不變性的頻率域加密方法應可以抵抗幾何轉換等攻擊；而該研究目前只在顯示其加密影像在印列輸出並掃描回數位檔案時仍具有浮水印驗證的功能，印列與掃瞄影像還需作影像定位的校準，並不能抵抗幾何攻擊方面。其密碼驗證需保留原始加密影像，與待解碼的浮水印影像作相關性比對以達驗證目的，必須保留原始加密影像是該研究在實際應用上的一大限制。

綜合分析相關印列圖像加密之研究的優劣性可以表1.1所示，對於裁切、幾何轉換、共謀攻擊、以及印列輸出時受到網點擴張的影響之比較與分析。

影像加密方法 抵抗攻擊	Hel-Or [8]	Fu(2002) [3]	Tseng [20]	Fu(2004) [4]	Kacker [10]
(1)裁切	**X**	**X**	**X**	**O**	**X**
(2)裁切與旋轉的幾何轉換	**X**	**X**	**X**	**X**	**X**
(3)共謀行為	**X**	**X**	**O**	**O**	**O**
(4)網點擴張	**X**	**X**	**X**	**X**	**O**

表 1.2 比較相關影像加密研究之優劣性

(1) 裁切攻擊：在不經旋轉、縮放的幾何變化下取得部份影像內容，[8][3][20]與[10]經裁切後喪失影像定位資訊即無法順利解碼；[4]的加密受限於影像內容，在裁切後的部分影像內容必須具有足夠密碼資訊的前提下，可達到解碼驗證的目的。

(2) 裁切與旋轉的幾何轉換攻擊：加密影像在經裁切喪失定位資訊後再經旋轉，這五種方法都無法因應這種幾何攻擊問題。

(3) 共謀攻擊[26]：[3]將密碼藏在特定位置，[8]利用兩個臨界值矩陣產生影像，在事先知道藏密方法的情況下，可透過蒐集加同一種密碼但不同內容的影像，以逆向工程統計出可能加密的位置以及密碼；[20][4]與[10]的加密位置受影像內容而改變，不易受到共謀攻擊。

(4) 網點擴張：避免印列輸出後鄰近的網點混合在一起不易辨識。[10]已模擬實際印列輸出的效果考量在加密技術中，因而可輸出高解析度影像不受影響；其他研究則受網點擴張影響甚鉅，在影像解析度必須有所限制。

1.3 論文綱要

為了解決先前半色調影像加密技術的限制，本研究在於提出一以網點為基礎的創新影像加密方法，以供印列輸出作底紋影像之應用為目的。本研究提出將隨機點分布的圖樣作為加密資訊，以其反覆的幾何變換與部份重疊來形成數位浮水印影像，而此密碼圖樣的幾何變換同時也可視為一種繪圖筆刷來描繪出影像的階調與輪廓，本研究具有以下特色：

(1) 加密後的半色調影像可供輸出的應用。本研究在製作上考量印列輸出後網點擴張的影響，避免墨點與墨點之間相鄰距離太過接近造成不易辨識的效果，因而可輸出高解析度的影像，並且在印列與掃描回數位檔案後，還可辨識出密碼；

(2) 在加密影像產生過程中，可混搭代表不同鍵值的密碼圖樣藏入，且密碼圖樣的幾何變換過程中也增添了許多隨機參數，不但提高編碼的複雜度，也適合與數位印刷設備結合產生每張加密資訊不同的高解析度影像；

(3) 本研究可利用將印列輸出的加密影像以掃描或其他取像方式重建數位影像予以解密，達到自動化機器閱讀的目的，而且不需要精準的定位，只需取得部份適當解碼區域，以部分對應的方法即可解決定位與密碼驗證的問題，同時解決了以往研究在影像定位與裁切、與旋轉等幾何轉換問題。

(4) 雖然是基於隨機圖樣本身設計的缺陷，無法達到擬真影像的目的，加密後的影像較淺可供底紋影像之應用，而且密碼圖樣可視為一種繪圖筆刷，以其幾何變換與部份重疊形成的加密影像具有非擬真影像(Non-Photorealistic Image, NPI)的視覺效果。

1.4 論文架構

第一章進行本研究動機與目的之簡介，以及數位網點種類與特性、資料隱藏與半色調影像加密研究的相關文獻之回顧與比較，並簡介本論文大綱與架構；第二章提出以隨機點分布的幾何轉換形成底紋影像之加密方法與驗證方式；第三章以隨機點分布的幾何轉換形成有意義的影像；第四章實驗結果與討論；第五章結論；第六章未來工作。