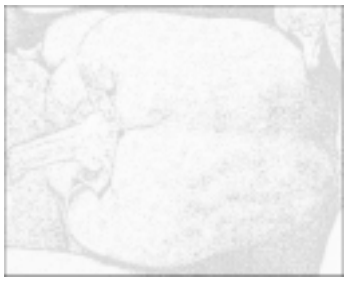
第四章、實驗結果與討論

4.1 裁切與旋轉的幾何轉換

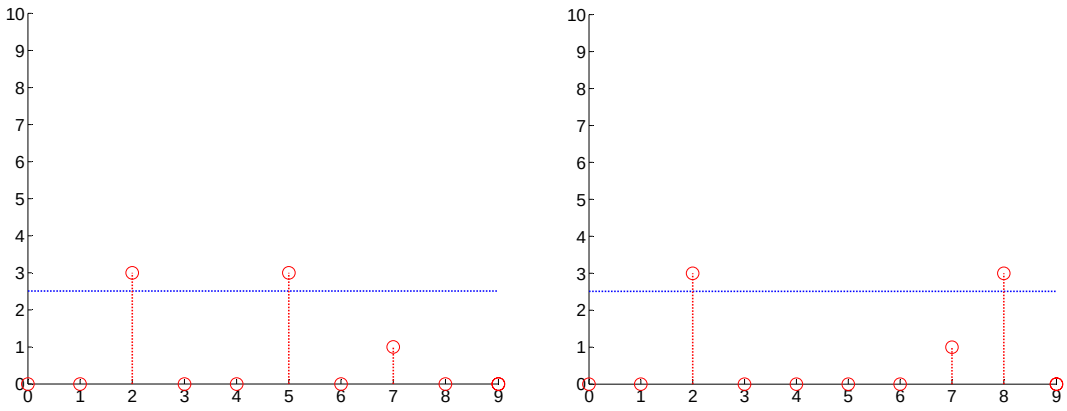
本研究中加密影像以影像解析度 720*dpi*，並以 Epson STYLUS C65 噴墨印表機以最高品質印列輸出(5760×1440*dpi*)，再由掃描器以 1440*dpi* 重建回數位影像。在此以對掃描影像隨機取得部份影像作密碼驗證，模擬實際取像情況可能有旋轉與裁切的幾何轉換情形，如圖 4.1 所示，並以 3.7 之敘述選擇適當解碼區域作密碼驗證，任取 10 處可能有密碼的區域影像，每區域重複作 20 次隨機指定基底進行幾何雜湊的密碼驗證，針對不同鍵值所得到的反應如圖 4.2 所示，橫軸顯示不同鍵值，縱軸代表比對成功的次數。由此顯示本研究可解決裁切後並旋轉的幾何攻擊。

“2”&“5”



“2”&“8”

圖 4.1　加密影像經裁切與旋轉



“2”&“5” “2”&“8”

圖 4.2　對應圖 4.1 之驗證結果

4.2 影像加密與驗證效果

如 4.1 所敘述的輸出條件，以不同鍵值的密碼組成加密影像如圖 4.3 所示，本研究以對加密並印列輸出的文件進行掃描取像，並從中隨機選擇適當解碼區域進行密碼驗證，適當區域的判斷條件如 3.7 的敘述，先判斷任取的區域影像內的特徵值數量多寡，以避免取得沒有密碼存在之最濃階調。在任取 10 處可能有密碼的區域影像，每區域重複作 20 次隨機指定基底進行幾何雜湊的密碼驗證，分別對十個鍵值的驗證結果如圖 4.4，橫軸顯示不同鍵值，縱軸代表比對成功的次數。

“2”&“5”

“4”&“8”

“0”&“1”

“4”&“8”

“6”&“8”

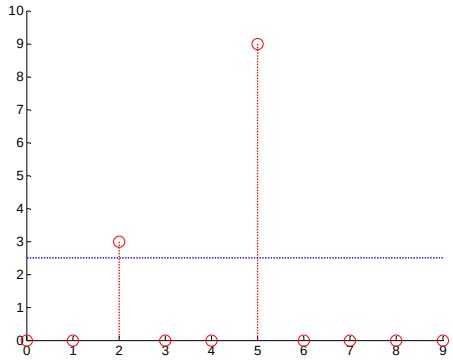
“3”&“9”

“2”&“8”

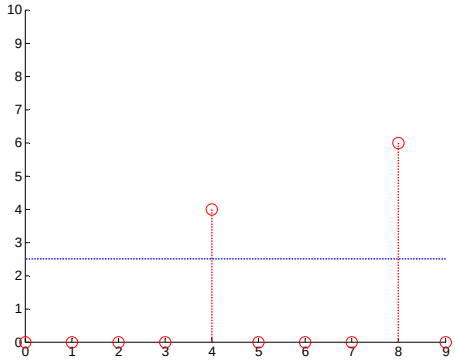
“0”&“1”

“4”&“6”

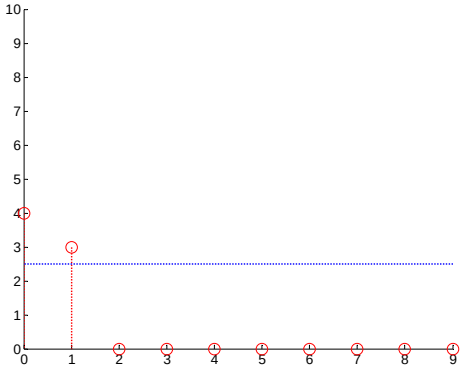
圖 4.3　加入不同鍵值的影像



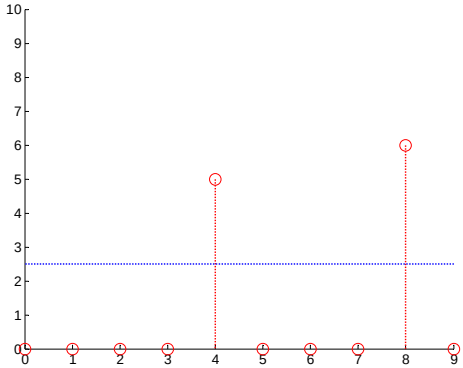
“2”&“5”



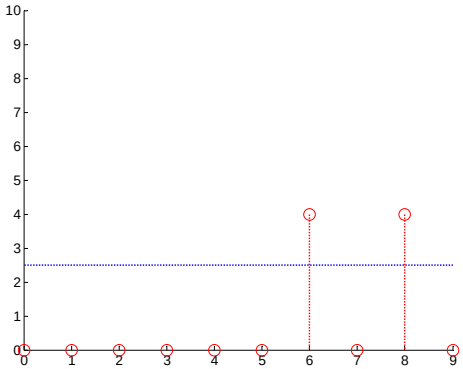
“4”&“8”



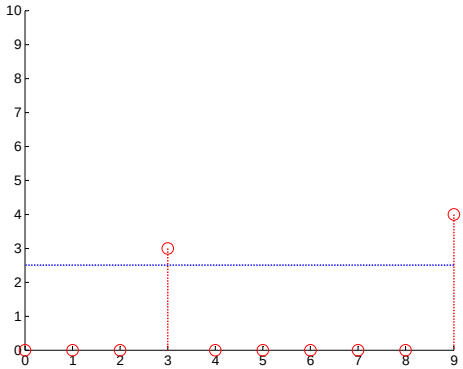
“0”&“1”



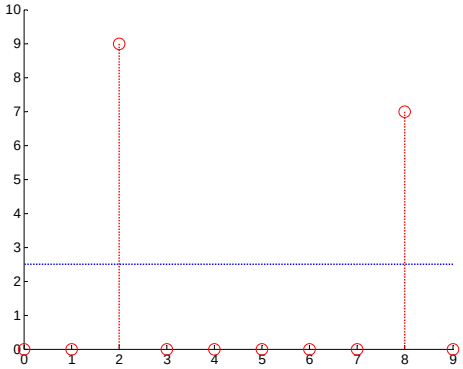
“4”&“8”



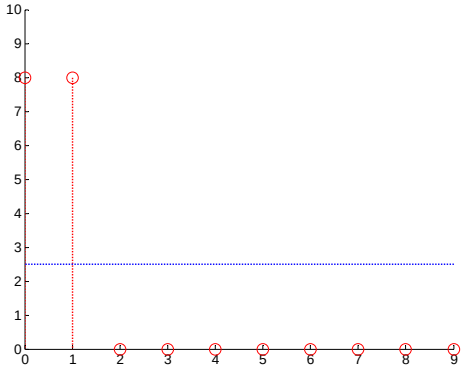
“6”&“8”



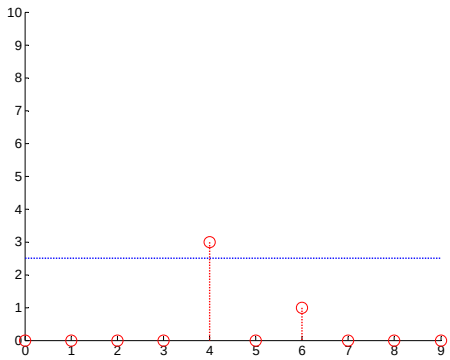
“3”&“9”



“2”&“8”



“0”&“1”



“4”&“6”

圖 4.4　對應圖 4.3 之驗證結果

在此展示灰階影像的藏密與驗證效果，分別以不同鍵值對不同影像的適當解碼區域做密碼驗證，在執行過 200 次的隨機指定基底進行幾何雜湊投票，一共得到的比對成功的總次數，超過藍色虛線的為驗證成功的結果，由圖 4.4 顯示驗證情形大致良好。而圖 4.3 加密影像表現出較淡色調，可做為底紋影像之應用，尤其其中三張同樣為 lena 影像，再加入不同鍵值的密碼圖樣後，在視覺效果上人眼觀察幾乎無差異，但藏有不同的鍵值也可提供相當的驗證效果，由此證明本研究適合搭配數位印刷設備產生每張藏有不同序號之影像，產生每張具有獨特密碼的影像，以達到版本控管之目的。

4.3 產生彩色加密影像

彩色印刷品是由不同色版(CMYK)的影像疊印而成，我們先將數位的全彩影像分成 CMYK 四個色版，每一色版都是一灰階影像，分別以上述加密方法，以密碼圖樣的幾何變換與部份重疊分別完成每一色版的加密影像，再合併成四色印列輸出，得到圖 4.5 的結果。而驗證過程，分別取得不同色版的影像進行幾何雜湊法對不同密碼圖樣作驗證，在整合不同色版的驗證結果，如圖 4.5 由不同鍵值混合所構成的加密影像，再由掃瞄器重建回數位影像，分別對每一色版的灰階影像進行以上驗證動作，即可驗證影像的真偽。

“4”&“5”

“0”&“1”

圖 4.5　將本研究應用於彩色影像之中

4.4 抵抗複製設備的偽造方式

本研究以輸出加密影像成文件為目的，而有心人士想要偽造文件時，可能透過掃描器與印表機輸出或複印機複印的方式得到偽造文件。本研究中的輸出條件為 720*dpi* 影像解析度，以 Epson STYLUS C65 噴墨印表機的最高品質印列輸出(5760×1440*dpi*)，訊號理論中，必須大於原始解析度兩倍以上的解析度，才能將原始資料完全重建，因而使用掃描器 1440*dpi* 重建其數位檔案，而非專家的有心人士可能直接以該數位檔案再印列輸出的方式來製作偽造文件，並且以目前桌上事務型掃描機最高解析度輸出(5760×1440*dpi*)，再重新使用 1440*dpi* 掃描解析度重建數位檔案與以解密時，其方式如圖 4.6 所示，而驗證結果顯示在這樣的條件是下無法通過驗證的。探究其原因是因為，利用掃描器取像則為類似執行反過網(inverse halftoning)的方式取得文件的數位影像(灰階影像)，而再以印表機輸出前此影像又透過過網產生二階影像印出成文件，在此反覆的處理過程與過網時的誤差擴散影響使得加密文件經掃描與印列後密碼不復存在，而無法通過密碼驗證。另外使用影印機的方式複製文件，也會因影印機本身的解析度限制對但區域的點取樣不足，而無法將密碼複製。

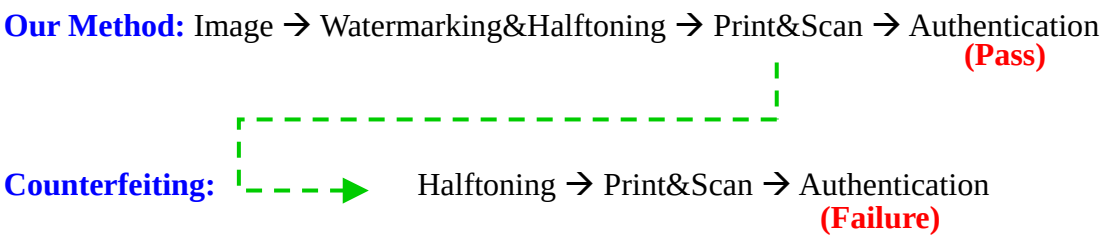


圖 4.6 本技術流程與可能遭受到的偽造方式