SVM 在列印掃描影像防偽之應用

王清林* 陳同孝** 盧瑞鵬**

*國立勤益技術學院資訊管理系

clwang@chinyi.ncit.edu.tw

**國立台中技術學院資訊管理系

tschen@ntit.edu.tw pon@isdn.com.tw

摘要

影像權益的問題日趨重要，如何快速且有效率的達到影像權益保障的目的是目前相當重要的議題。SVM (Support Vector Machine) 是一套相當新穎的分析工具，該工具利用統計學上的分類（Classification）與回歸（Regression）等觀念，對我們所要探討的任何問題，都能夠做出精準且詳細的分析與預測，在本篇論文中，我們運用 SVM 來解決影像權益保障的問題，利用影像中的特徵值當作 SVM 訓練的資料，透過 SVM 的分析之後，可得到資料的分佈與趨勢，將來在進行影像防偽的工作時，我們可以套用已得到的資料分佈與趨勢，對我們認為可能遭竄改的影像做偵測分析。經過我們的實驗分析結果，SVM 可以正確且快速的指出影像中遭偽造的區域，這對於影像權益保障的問題，是個相當不錯且有效率的解決方式。

關鍵字：SVM, 特徵值, 影像防偽

一、前言

拜網際網路發展快速之賜，拉近了人與人溝通的距離。大量的數位影像被廣泛地應用於網際網路上，如何確保數位影像的安全是目前相當重要的議題。目前對於數位影像的保護大部分是利用浮水印（Watermark）的技術來達成[1][2][4]，且利用浮水印的技術亦可達到權益保障（Authentication）的目的[1][2][10]，而浮水印的技術又可依照其特性分成可視（visible）[2]與不可視（invisible）[1][4]兩種，可視的浮水印通常採用有意義的圖示嵌入數位影像中進而達到影像保護的目的，例如公司行號的標記或是特殊的標記，而此種浮水印直接由肉眼就可以清楚辨別；不可視的浮水印則須利用某些特定的演算法，才能夠將浮水印藏入數位影像中，而取出浮水印時也須透過特定的演算法，此種浮水印則無法直接由肉眼觀測出，若將來發生權益糾紛問題的時候，我們可以從原始影像中取出預先藏入的浮水印來做驗證，目前浮水印技術討論的範圍皆是在電腦中做處理，而忽略數位影像列印後的保護，當數位影像需要做列印輸出時，藏入的浮水印必須

要能夠抵抗列印及掃描的嚴重失真，因此浮水印的強韌性就受到很大的考驗。Support Vector Machine（SVM）是目前相當新穎的一套統計分析工具，該工具利用統計學上分類（Classification）與回歸（Regression）的概念，來解決圖形辨識與決策理論的問題，我們可以利用該軟體所產生的模組（Model）來進行影像竄改分析的工作，本篇論文著重在列印後掃描影像竄改之偵測，並利用 SVM 工具來提供一整套有系統的分析流程，因此，我們除了利用不可視的浮水印技術預先藏入浮水印，將來利用藏入的浮水印以及擷取列印後掃描影像的特徵來進行分析的工作，經過實驗發現，利用 SVM 來進行列印後掃描影像竄改的分析工作，除了可以提供一套完整有系統且快速的分析流程之外，亦可達到相當不錯的效果。

本篇論文的架構如下，第一節是前言，第二節是回顧過去相關的研究，第三節為本篇論文所用的技術簡介，第四節為本篇論文所提出的方法與流程，第五節為實驗的結果與分析，第六節為本篇論文結論，最後附上本篇論文所參考的相關資料。

二、相關研究回顧

目前對於影像安全的防護，大多是在數位影像中藏入浮水印，而藏入浮水印的方法又可分為兩種，一種是直接針對空間域（spatial domain）影像的像素值做修改[2]，進而達到藏入浮水印的目的，此種方法的優點是方法簡單、修改容易，利用這種方法藏入浮水印對於破壞的抵抗較弱，且若處理不當則很容易就可由肉眼辨識出被修改的部位；另外一種方法則是先將影像由空間域轉換至頻率域（frequency domain），然後再針對頻率域影像做修改[1][4]，頻率域影像是以高低頻帶來呈現，由於人類的眼睛對於低頻區域較為敏感，而對於中高頻區較為不敏感，我們可以利用這種特性並針對頻率域影像中的中高頻區做少量的修改，再轉換至空間域影像，利用這種方法藏入的浮水印以人類的肉眼是不容易辨識出來的，而且其抵抗破壞的能力會優於直接在空間域修改的方法，若影像利用[1][2][4]的方法保護影像，雖然都可以達到不錯的效果，但都不適用於列印掃描後的影像，陳同孝、林泉成提出的方法[6]可達到列印掃描影像的保護，但卻有下列幾項缺點，1.藏入特徵值的區塊需要事先做選擇，所以該區塊必須紀錄，造成使用上的不便。2.為了抵抗列印掃描的失真破壞而藏入的三份特徵值雖可提升資料容錯的能力，但特徵值本身並無錯誤更正能力，所以資料的正確性不高。3.無法明確地指出影像遭受竄改的部位，需要由使用者自行判斷影像是否遭到竄改，若無原圖做為參考則很難判定影像是否有遭受到竄改。4. 在影像防偽的工作上無法提供一套完整且有效率的方法。為了改進上述的缺點，我們的做法在藏入特徵值的順序是從左而右，由上而下循序藏入，不需要選取特定的區塊，因此也不必紀錄藏入特徵值的區塊位置，並利用 RS Code [3][5]對特徵值進行編碼，使得藏入的特徵值具有錯誤更正的能力，以提高資料的正確性，最後利用了 SVM 對資料進行一套完整的分析工作，我們會預先透過 SVM 對列印掃描後的影像做分析訓練，並由 SVM 產生一套模組，將來透過這個訓練出來的模組對列印掃描後的影像做分析，並可指出影像中遭受竄改的部位。

三、相關技術簡介

SVM（Support Vector Machine,）

SVM 是一套相當新穎的分析工具，該工具利用統計學上回歸（Regression）、分類（Classification）等觀念[9][6]，用來解決圖形識別與決策理論的問題，在本篇論文中，我們利用 SVM 工具來分析資料，以期達到列印後掃描影像竄改之偵測。

回歸（Regression）

當 $Y = aX$ 時，我們可以稱 Y 是 X 的函數，即當 X 的值決定時，Y 值也會一定，可是有的時候 X 的值雖決定，但 Y 的值卻仍然無法很正確的決定，雖然是這樣，但也不可以說 X 與 Y 兩者之間完全無任何的關係存在，例如當知道母親身高的時候並沒有辦法正確地求得子女的身高，這主要是因為母親身高與子女身高關係並不能夠以函數式來表示，但我們卻可知道當母親身高較高時，其子女的身高也會有比較高的傾向，反之，若是母親身高較矮時，其子女的身高也會有比較矮的傾向，所以可得知，母親的身高與其子女的身高並不能說是完全無關係的。

因此，若我們把變數 X 與 Y 之相對數據（X_1,Y_1），（X_2,Y_2）.....（X_n,Y_n）的 n 組數據在橫軸取 X 值，縱軸取 Y 值，並把 n 個點畫在座標上時，可得如下圖的散佈圖。

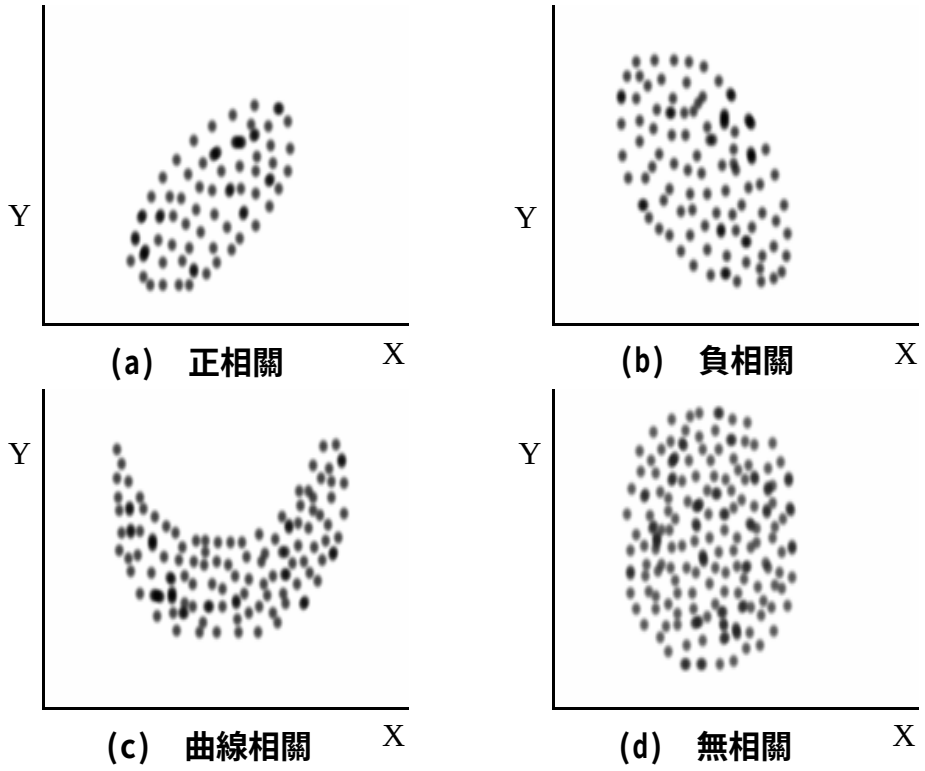


圖 1. 散佈圖

我們可以從上圖觀測出，X 與 Y 的值可能會有四種不同的關係存在，即正相關、負相關、曲線相關與無相關四種，若對於散佈圖做直覺的判斷時，常常會有判斷錯誤的情形發生，即本來為無任何相關關係的事物，而誤判為有相關，而本來有相關的則判為無相關，

假設我們不只是要獲得兩種以上觀測值間的關係，而是想要更進一步地對 X 與 Y 之間的關係利用函數式表示出來，此一方法即稱為回歸分析。

分類（Classification）

在一群資料中，我們可以針對該群資料的特性與分佈將一群資料分成多個子集合，每個子集合內的元素皆有相似的特性，如下圖所示：

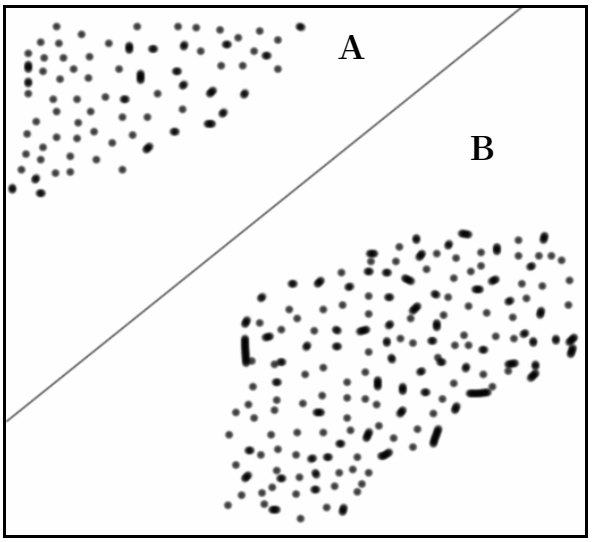


圖 2. 分類圖

上圖中黑點表示資料在空間上的分佈情形，從上圖中可以清楚的看到可分為 A、B 兩大類，我們可以利用分類的觀念來對資料進行分類的工作，以利資料分析的工作，在本篇論文中，我們將影像資料分成遭受竄改區域與未遭受竄改區域兩類，並利用 SVM 來進行訓練的工作。

代表性（representability）

有一群資料分佈圖如下：

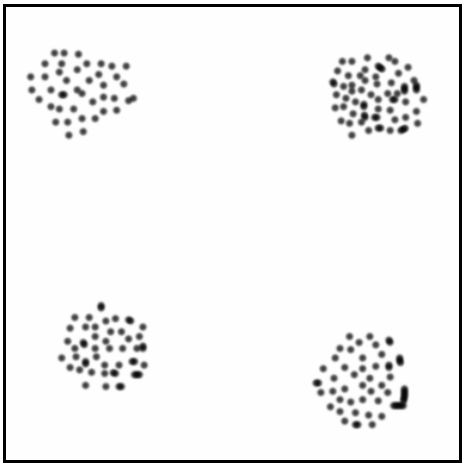
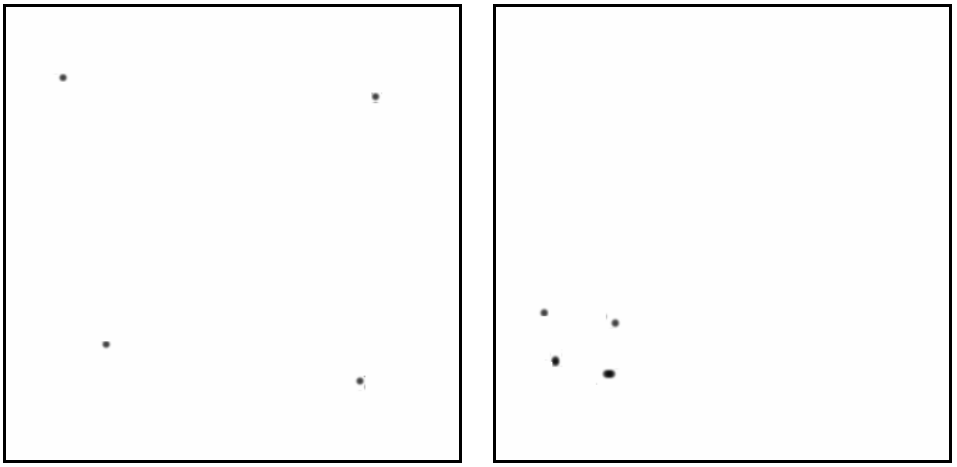


圖 3. 資料分佈圖

若今欲以四點來代表這一群資料的分佈情況，考慮下列圖所示：



(a) (b)

圖 4. 資料分佈代表圖

我們可以由上圖中發現.圖 4.(a)較.圖 4.(b)較具有代表性，在圖 4.(a)中的四個點分別為圖中四個小群中的點，因此若以四個點代表資料的分佈，則較具有代表性，反之，圖 4.(b)中的四個點為圖中四個小群其中一群所取出的四個點，因此若以此四點來表示整群資料的分佈，則代表性會較圖 4.(a)差，在本篇論文中使用 SVM 來分析資料，因此資料是否具有代表性會影響整體的效果，若是訓練的資料代表性強，則訓練出來的 Model 的效果也會較佳，即進行竄改偵測的工作所得到的結果也會較好；反之，若是訓練的資料代表性較弱，其訓練出來的 Model 的效果也會較差，即竄改偵測的工作所得到的結果會較不理想，因此，若欲利用 SVM 進行分析的工作，需特別注意所訓練的資料是否具有足夠的代表性，代表性的強弱會直接影響效果的好壞。

離散餘弦轉換（DCT）

離散餘弦轉換可將影像由空間域轉換至頻率域，公式如下：

$$D(i,j)=\frac{1}{\sqrt{2N}}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{(2x+1)ip}{2N}\right]\cos\left[\frac{(2y+1)jp}{2N}\right] \quad (1)$$

$$f(x,y)=\frac{1}{\sqrt{2N}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}C(i)C(j)D(i,j)\cos\left[\frac{(2x+1)ip}{2N}\right]\cos\left[\frac{(2y+1)jp}{2N}\right] \quad (2)$$

上式中 $f(x,y)$ 為空間域像素的位置，$D(i,j)$ 為頻率域的係數位置，而 $C(i)$ 及 $C(j)$ 則隨著 i,j 的變化而改變，當 i 等於 0 則 $C(i)$ 為 $\frac{1}{\sqrt{2}}$，當 j 等於 0 則 $C(j)$ 為 $\frac{1}{\sqrt{2}}$；當 i 不等於 0 則 $C(i)=1$，當 j 不等於 0 則 $C(j)=1$，公式(1)又稱為離散餘弦正轉換（Forward Discrete Cosine Transformation, FDCT），即將影像由空間域轉換至頻率域；若需要把頻率域的資料轉換至空間域的資料時則須利用公式(2)，又可以稱為離散餘弦反轉換（Inverse DCT, IDCT）。數位影像在頻率域中是以高低頻帶的方式來呈現，由於人類的眼睛對於影像的低頻區域較為敏感，而對於中高頻區域較不敏感，我們可以利用這種特

性藏入特徵值，未來我們將利用這個預先藏入的特徵值來進行分析的動作。

Reed-Solomon Code（RS Code）

我們採用 RS Code 來提高浮水印的正確性，RS Code（n,k,t）是一種週期性（Cyclic）的錯誤更正碼[5]，其中：

n ：經 RS Code 編碼過後的長度

k ：編碼長度

t ：錯誤更正的能力

RS Code 每次會取長度為 k bits 進行編碼的動作，編碼後的長度為 n bits，且每 n bits 當中有 t bits 的錯誤更正能力，三者關係式為：

$$n = k + 2t \qquad (3)$$

四、方法與流程

SVM 工作流程圖如下：

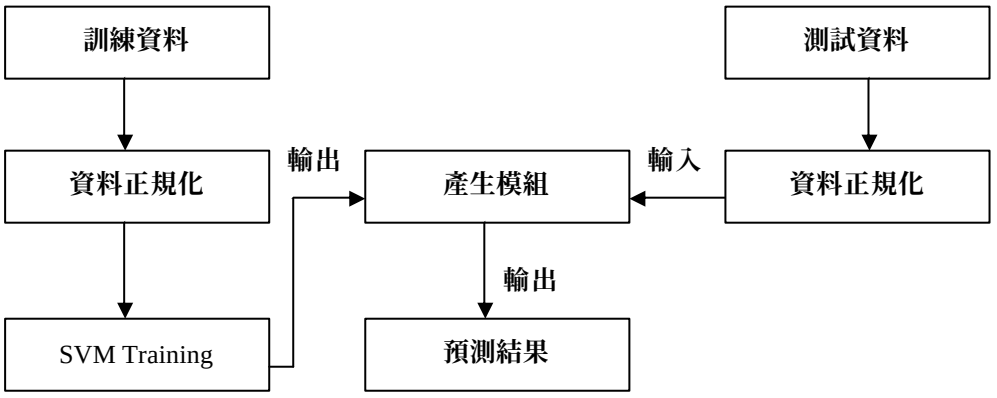


圖 5. SVM 工作流程圖

由上圖可以得知，我們必須先輸入已知的資料讓 SVM 進行分析的工作進而產生對應的模組，將來以模組當作分析的依據對測試資料進行分析，若欲訓練出一個較為良好的模組，則訓練資料就顯的相當重要，若是能夠提供較完整且正確的訓練資料，透過 SVM 所產生出的模組就會有比較良好的效果，因此在本篇中我們利用影像的邊緣值當作特徵值藏入數位影像的頻率域當中，在影像經過列印掃描後，再將藏入的特徵值取回並輸入至 SVM 做訓練。

藏入特徵值的流程圖如下：

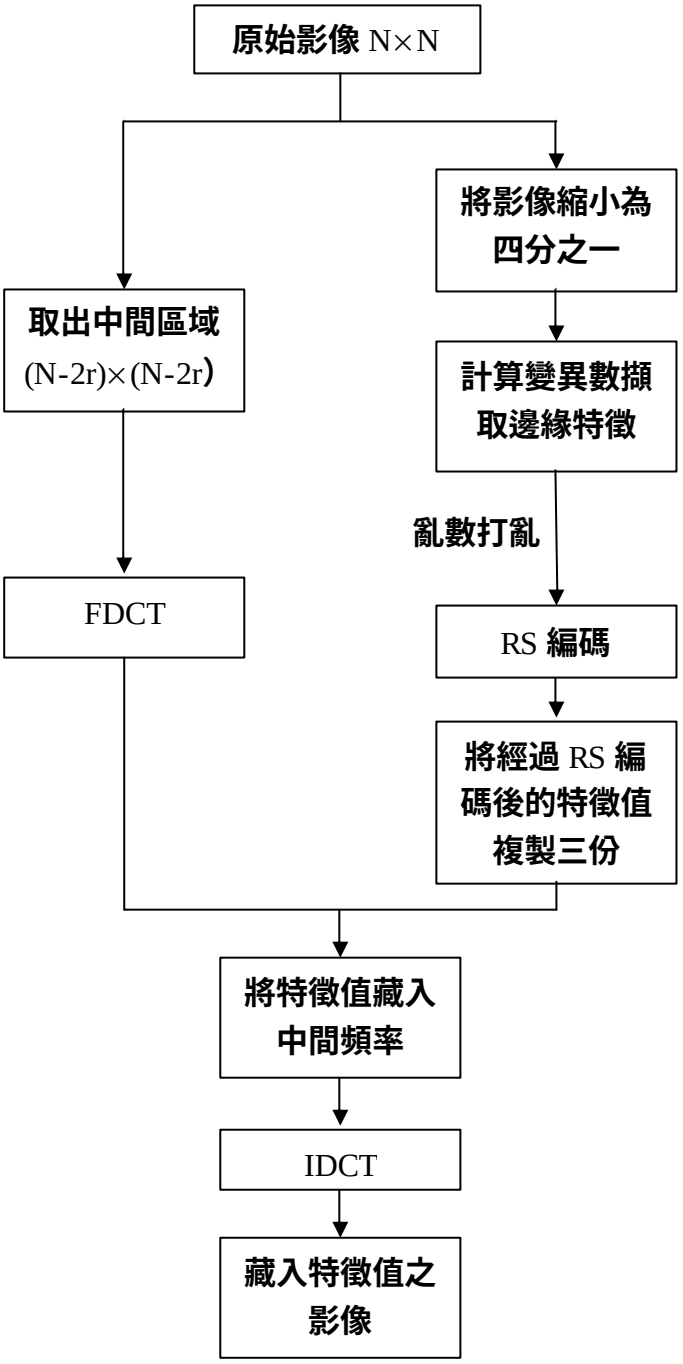


圖 6. 特徵值藏入流程圖

若一張影像為 N×N, 首先將影像縮小為原圖的四分之一, 然後將影像切割成大小為 4×4 且不重疊的區塊, 然後利用統計學上變異數的計算公式計算出每個區塊的變異數, 公式如下：

$$Variance = \frac{\sum_{i=1}^{l}(x^i - \bar{x})^2}{l} \qquad (4)$$

上式中，x 為該區塊中每一點的像素值，$\bar{x}$ 為該區塊像素平均值，l 為區塊大小，當該區塊所計算的變異數大於我們訂定的門檻值時，即認定該區塊為有邊緣通過的區塊，則輸出 1；當該區塊所計算的變異數小於門檻值時，即認定該區塊為平滑區域，則輸出 0。我們必須訂定一個適當的門檻值，因為當門檻值設定太小所偵測出的邊緣資訊會太多；反之，當門檻值設定太大，則偵測出的邊緣資訊會太少，在本篇論文中我們以邊緣資料當作特徵值藏入原始影像中，並利用 SVM 對藏入的特徵值進行分析進而產生模組，將來利用此模組即可對列印掃描後的影像進行分析並指出影像中遭竄改的部位，進而達到影像防偽的工作，下圖為變異數示意圖：

圖 7. 變異數示意圖

為了提高邊緣特徵的安全性，在藏入這些邊緣特徵之前我們必須將邊緣特徵的順序打亂，我們的做法是先給定一個亂數種值給亂數產生器使其可以產生一連串的數值，然後再根據這一連串的數值重新排列邊緣特徵的順序，將來在還原的時候再利用相同的亂數種值重新排列還原成原始的順序，為了讓藏入的邊緣特徵能夠有錯誤更正的能力，因此我們利用 RS Code 對藏入的特徵值進行編碼，又為了能夠加強邊緣特徵的正確性與容錯率，我們必須把這個經過 RS 編碼後的特徵值複製成三份，將來我們可以透過交叉比對的方式將三份資料整合成一份，藏入三份資料的好處是當其中一份資料發生錯誤時還可以比較其他兩份相同的資料，可以大大的提高資料的正確性，若只藏入一份邊緣特徵，如果發生錯誤的情形則沒有比較的依據。我們都知道數位影像在經過列印及掃描後對於影像的色階以及亮度都會造成很嚴重的破壞，其破壞的程度還會受到硬體設備的等級以及人為不當的操做方式所影響，為了能夠讓竄改偵測的工作能在一般的周邊設備進行且為了提高取出的特徵值的正確率，所以利用 RS 編碼以及將特徵值複製成三份的方式藏入資料，在本篇論文中，我們評定特徵值的正確率乃是採用偵測竄改區域成功百分比、錯誤百分比以及總體正確率三種判定方法，其公式為：

偵測竄改區域成功百分比 = (偵測竄改成功總數 / 遭竄改區塊總數)×100 (%) (5)

錯誤百分比 = (未遭受竄改區域誤判總數 / 未遭受竄改區塊總數)×100 (%) (6)

總體正確率 = ((總區塊數 - 錯誤區塊數) / 總區塊數)×100 (%) (7)

由上述三式可以看出，偵測竄改區域成功百分比越高，則偵測出影像中遭竄改的區域越

多；錯誤百分比越低，則未遭受竄改的區域遭誤判的機率越低；而總體正確率則可以看出一張影像的總體狀況，同樣地，當總體正確率越高時則表示不但竄改區域能夠準確的判斷出，而且誤判的程度會越低。

接下來要選擇特徵值所要藏入的位置，為了能夠提升取出的特徵值的正確率，因此我們只取中間區域進行離散餘弦轉換，作為藏入特徵值的區域，範圍如下圖 8.(b)所示，圖 8.(a)中黑色實線所框選的區域即是中間區域。

(a) $N \times N$　　(b)（N-2r）×（N-2r）

圖 8. 影像中間區域

我們的做法是取一張影像的中間區域進行離散餘弦轉換的工作，然後我們選擇經過離散餘弦轉換後每個區塊的中間頻率作為藏入特徵值的位置，如下圖 9.所示：

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

圖 9. 頻率域藏入位置

藏入特徵值的順序為由左到右由上到下循序藏入區塊中，為了讓藏入的特徵值能夠抵抗列印掃描的失真，我們採用階段性的方式藏入特徵值，我們會設定一個區段（Step）並根據特徵值的不同以及預藏入的頻率域係數值正負的不同根據下列公式做不同的修改，公式如下：

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor \times STEP\right) + \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor \bmod 2 = 0, DCT_{ij} > 0, C_i = 0 \tag{8}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor + 1\right) \times STEP + \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor \bmod 2 \neq 0, DCT_{ij} > 0, C_i = 0 \tag{9}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor \times -STEP\right) - \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor \bmod 2 = 0, DCT_{ij} < 0, C_i = 0 \tag{10}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor + 1\right) \times -STEP - \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor \bmod 2 \neq 0, DCT_{ij} < 0, C_i = 0 \tag{11}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor + 1\right) \times STEP + \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor \bmod 2 = 0, DCT_{ij} > 0, C_i = 1 \tag{12}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor \times STEP\right) + \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{STEP} \right\rfloor \bmod 2 \neq 0, DCT_{ij} > 0, C_i = 1 \tag{13}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor + 1\right) \times -STEP - \left\lfloor \frac{STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor \bmod 2 = 0, DCT_{ij} < 0, C_i = 1 \tag{14}$$

$$DCT_{ij} = \left(\left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor \times -STEP\right) - \left\lfloor \frac{-STEP}{2} \right\rfloor \quad , \; if \quad \left\lfloor \frac{DCT_{ij}}{-STEP} \right\rfloor \bmod 2 \neq 0, DCT_{ij} < 0, C_i = 1 \tag{15}$$

$$if \quad \left\lfloor \frac{|DCT_{ij}|}{Step} \right\rfloor \bmod 2 = 0 \quad \text{then} \quad C = 0, \text{ else } \; C = 1 \tag{16}$$

式中DCT_{ij}為挑選出的頻率域係數值，C_i為預藏入的特徵值，無論經過任何一個公式修改，最後該頻率係數值都會修改成對應區段的中間值，假設區段大小為 15，當我們要藏入的特徵值為 1，且該頻率域係數值為正數 +5 且 $\left\lfloor \frac{+5}{Step} \right\rfloor \bmod 2 = 0$ 帶入公式(12)，$\left(\left\lfloor \frac{DCT_{ij}}{Step} \right\rfloor + 1\right) \times Step + \left\lfloor \frac{Step}{2} \right\rfloor = \left(\left\lfloor \frac{5}{15} \right\rfloor + 1\right) \times 15 + \left\lfloor \frac{15}{2} \right\rfloor = +22$；當我們要藏入的特徵值為 0，且未頻率域係數為負數 -5 且 $\left\lfloor \frac{-5}{-Step} \right\rfloor \bmod 2 = 0$ 帶入公式(10)，$\left\lfloor \frac{DCT_{ij}}{-Step} \right\rfloor \times -Step - \left\lfloor \frac{Step}{2} \right\rfloor = \left\lfloor \frac{-5}{-15} \right\rfloor \times (-15) - \left\lfloor \frac{15}{2} \right\rfloor = -7$，重複上述步驟就可將特徵值藏入頻率域係數之中，當我們要取出特徵值時，套用公式(16)將修改過後的頻率域係數值帶入 $\left\lfloor \frac{|DCT_{ij}|}{Step} \right\rfloor \bmod 2$，我們可以得到 $\left\lfloor \frac{|+22|}{15} \right\rfloor \bmod 2 = 1$，$\left\lfloor \frac{|-7|}{15} \right\rfloor \bmod 2 = 0$，最後得到的 0 與 1 就是我們當初藏入的特徵值，設定一個區段主要的目的是為了讓影像在經過列印掃描後，能夠有容許誤差的範圍而設定的區段的大小就是容許誤差的大小，如圖

10.所示，不過值得注意的是，雖然將區段設定成較大的範圍可以有較佳的容錯率，但區段範圍設定過大時，也正意味著影像將會受到較為嚴重的破壞，相對地影像品質就會比較差，反之若將區段設定成較小的範圍，雖然會得到品質較佳的影像且較接近原始影像，但會降低特徵值對於列印掃描失真破壞的抵抗能力，故取出特徵值的正確率會較低即容錯率較低，所以在特徵值的容錯率與影像品質上我們必須做取捨。

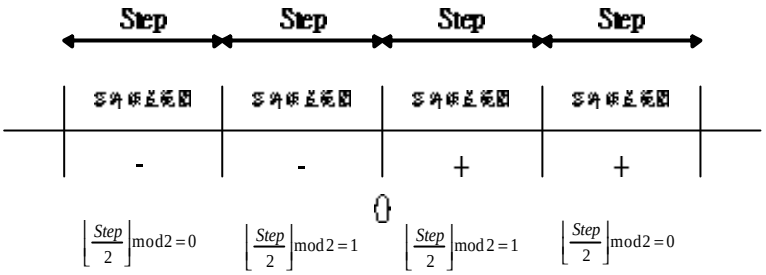


圖 10. 係數修改示意圖

特徵值取回流程圖如圖 11。

我們先將列印後的影像經由掃描器輸入至電腦中，同樣地取出影像的中間部分進行離散餘弦轉換，依照圖 9.的位置將每個區塊中對應的頻率域係數一一取出，然後將取出的頻率域係數值分別帶入公式(16)中，如果該頻率域係數帶入公式(16)計算後的值等於 0，則表示當初我們藏入的特徵值為 0，反之若該頻率域係數帶入公式(16)計算後的值等於 1，則表示當初我們藏入的特徵值為 1，重複上述步驟就可以將預先藏入的特徵值完全地取回，由於我們藏入的特徵值有三份，所以必須將三份特徵值整合為一份，我們的做法是，假設藏入的資料為 ABC 三份，我們的做法是當 B 資料等於 C 資料的時候，修改 A 資料的內容使得 A 資料等於 B 資料，當 B 資料不等於 C 資料時，則 A 資料不做任何修改，重複上述動作，當完成所有的比對後 A 資料就是三份資料交叉比對的結果，然後再將 A 資料做 RS Decode，完成 RS decode 的工作後我們會得到更正過的特徵值，再利用相同的亂數種值產生一連串的數值，再根據這一連串的數值就可以還原特徵值原本的排列順序，接下來我們將列印掃描後的影像縮小成原圖的四分之一，同樣地利用變異數公式(4)計算變異數取出邊緣資料。

接下來必須進行資料正規化的工作，我們必須根據 SVM 所提供的格式來對資料做正規化的工作並輸入至 SVM 以便產生我們所需要的模組，在本篇論文中我們採用 mysvm2.0 版本，該 SVM 工具所規定的格式如下：

Value1 Value2 Value3.....Label

Value 為資料經過數值量化後的值，Label 為目標值，在本篇論文中我們設定兩組目標值，其中 1 為未遭受竄改區域；2 為遭受竄改區域，假設一訓練影像大小為 512×512，先將影像縮小為四分之一，即大小為 256×256，在此我們重新定義訓練影像中的區塊大小為 16×16，由於影像擷取邊緣特徵所設定之區塊大小為 4×4，故在 16×16 區塊大小中共有 16 個邊緣特徵值，我們以 8 個邊緣特徵值結合成為一個數字，從藏入的邊緣特徵以及列印掃描後所擷取的邊緣特徵，共可以得到四組數字，為了增加資料的代表性，

我們還必須計算大小為 16×16 區塊內的像素平均值以及變異數還有預先藏入的邊緣特徵與列印掃描後的邊緣特徵相似的百分比，用上述資料來當作訓練的資料輸入至 SVM 中訓練，如圖 12。

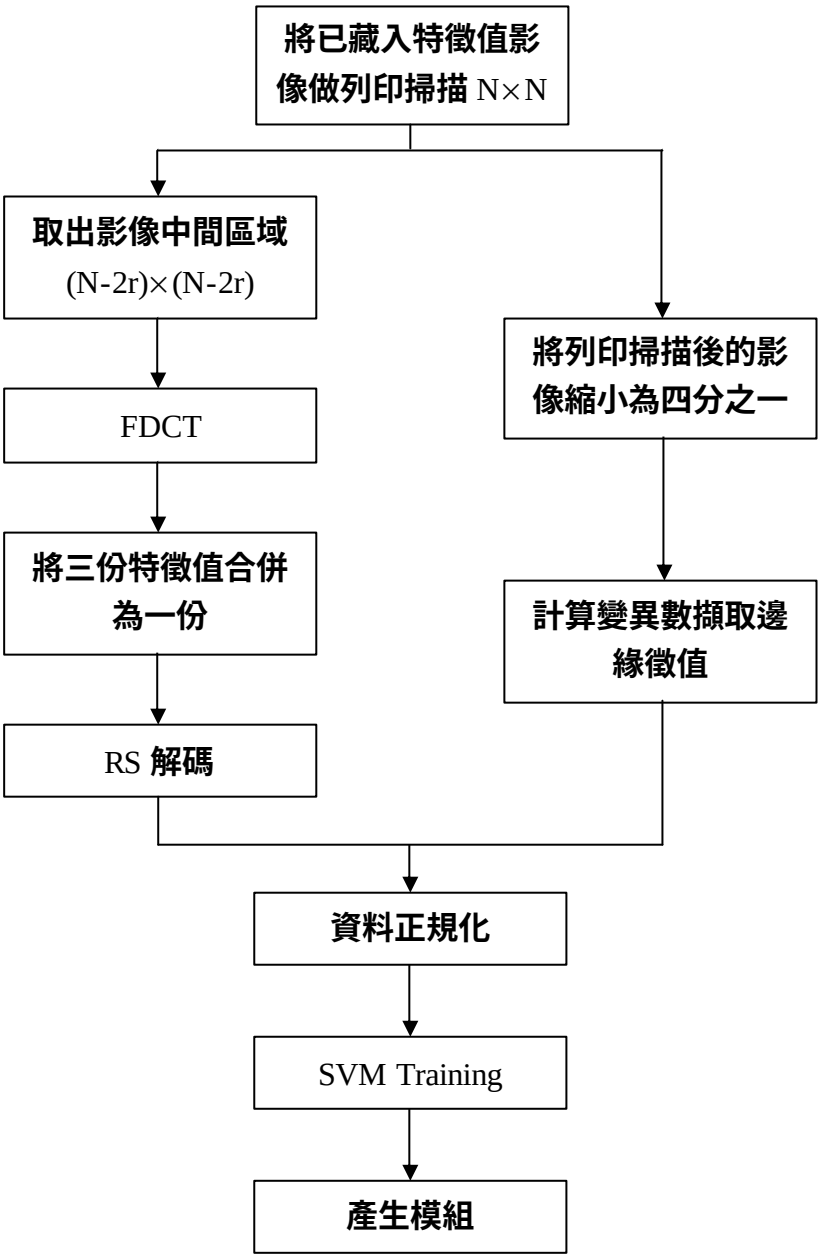


圖 11. 特徵值取回流程圖

圖 12 中的平均值與變異數所紀錄的數值為區塊大小 16×16，特徵值相似百分比由預先藏入的邊緣特徵與列印掃描後影像的邊緣特徵計算而得，由於計算邊緣特徵所訂定的區塊大小為 4×4 故在 16×16 區塊內共有 16 個邊緣特徵，即上圖中的數值 0 與 1，我們將每 8 個邊緣特徵結合成一個數字，故每 16×16 的區塊內可得兩組預先藏入的特徵值與兩組列印掃描後影像的邊緣特徵值，所以在一個 16×16 的區塊內共有 7 個數值來

描述該區塊，然後必須訂定目標值，訂定目標值的目的是告知 SVM 此大小為 16×16 的區塊是否有遭受到非法的竄改，重複上述步驟，當資料完成正規化後即可輸入至 SVM 作訓練。

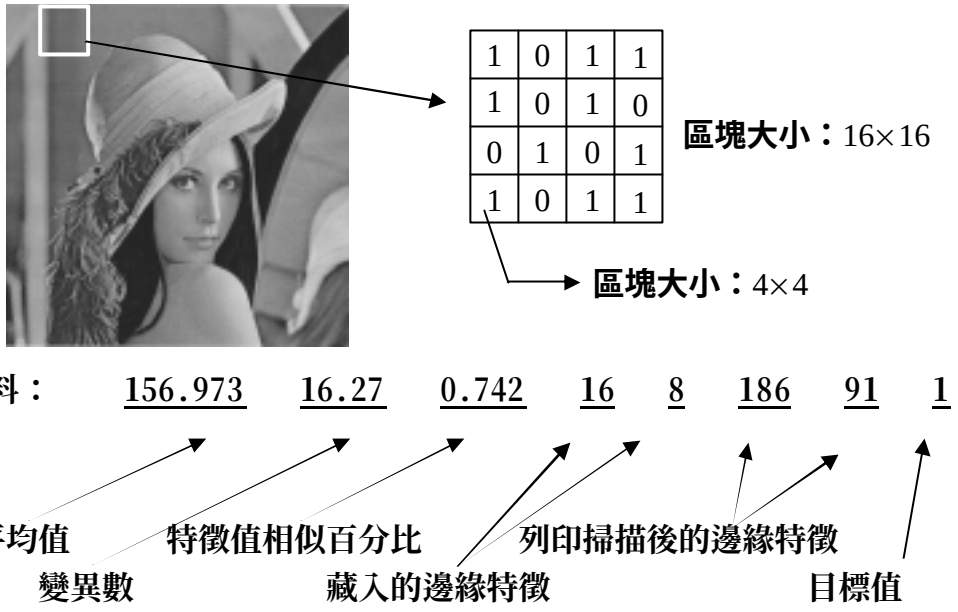


圖 12. 訓練資料格式

五、實驗分析

本論文所使用的實驗平台為：Pentium III 667 MHz 處理器、256MB RAM、作業系統為 Windows 2000、掃描器為 VUEGO 310P、印表機為 HP LaserJet 2100、程式撰寫工具為 Java 1.2.1，在 RS Code 的實做方面我們利用 Matlab R12 的內建函數以及採用 Ulead PhotoImpact 6.0 影像處理軟體，SVM 則採用 mysvm2.0 版作為實驗的輔助工具。利用 SVM 做預測之前必須先輸入已知的資料做訓練，由於我們的目的在於偵測列印掃描影像是否有遭受竄改，因此必須先定義遭竄改的影像並輸入至 SVM 訓練，在本篇論文中共使用九張 Lena 影像做為訓練資料，如下所示：

圖 13 中每張 Lena 的影像皆為列印後遭受竄改的影像，我們將利用這些影像的特徵值，透過 SVM 訓練來產生模組，原則上，若是訓練資料越完整則所產生的模組其代表性會較佳，即越能夠達到我們的目的，不過需要注意的是，若是訓練資料過大則訓練所要耗費的時間也越久，且若是訓練資料的代表性較差時，雖有大量的訓練資料，亦無法產生較佳的模組，故訓練資料的正確性與代表性為產生較佳模組的主要原因。

圖 13. 訓練資料

實驗一：

(a) 遭受竄改影像 (b) SVM 偵測結果

圖 14. 實驗結果 1

表 1. 偵測正確率

區塊總數	遭竄改區塊數	未遭受竄改區塊數	偵測遭竄改區塊數	誤判區塊數	偵測竄改區域成功百分比(%)	錯誤百分比(%)	總體正確率(%)
256	12	244	7	6	58.3 %	2.3 %	97.7 %

在實驗一中共有三處遭受到竄改，表 1.中列出實驗相關數據，我們可以發現利用 SVM 做分析預測時會有誤差的情況發生，這與在訓練模組時所輸入的訓練資料有關，如前文所述，若訓練資料的代表性及正確性越強，則在分析階段所會產生的誤差也會越小。由於實驗一中遭受竄改的圖形並不完全存在於訓練資料中，故透過 SVM 做分析預測時只能夠大約地預測出遭受竄改的位置，但我們從實驗中就可以發現到 SVM 的確具有分析預測的功能，且已能夠偵測出影像中遭竄改的區塊。

實驗二：

(a) 遭受竄改影像 (b) SVM 偵測結果

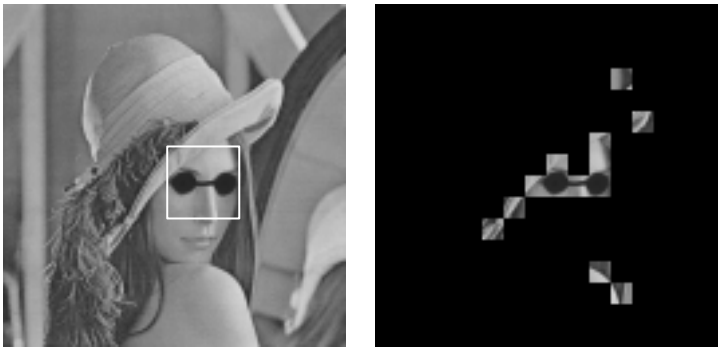
圖 15. 實驗結果 2

表 2. 偵測正確率

區塊總數	遭竄改區塊數	未遭受竄改區塊數	偵測遭竄改區塊數	誤判區塊數	偵測竄改區域成功百分比(%)	錯誤百分比(%)	總體正確率(%)
256	13	243	7	8	53.8 %	3.1 %	96.9 %

實驗二之相關數據如上表 2.所示。

實驗三：



(a) 遭受竄改影像　　(b) SVM 偵測結果

圖 16. 實驗結果 3

在實驗三中，其偵測竄改區域成功百分比與總體正確率均高出前兩個實驗，我們可以從訓練資料中觀察到其中有類似於實驗三的遭竄改影像，亦再一次的說明當訓練資料越具有代表性時，產生出的模組其效果就會越好。

表 3. 偵測正確率

區塊總數	遭竄改區塊數	未遭受竄改區塊數	偵測遭竄改區塊數	誤判區塊數	偵測竄改區域成功百分比(%)	錯誤百分比(%)	總體正確率(%)
256	4	252	4	9	100 %	3.5 %	96.5 %

六、結論

目前數位影像在網路上廣泛地被使用，安全性一直是重要的議題，尤其當數位影像需要做列印出的時候，其安全性更是堪慮，而我們所提出的方法能夠提供一整套有系統、有效率且可以指出列印後影像中遭受竄改的部位，利用 SVM 工具來進行竄改偵測的工作不但快速且簡單、方便，一般的使用者皆可使用 SVM 工具以及訓練出來的 Model 來進行竄改偵測的工作。相信在我們的方法保護下，能提供創作者更安全的創作環境，提高創作者創作的意願，且能有效地嚇阻未經授權的非法行為，而無需擔心創作遭到不法的竄改。

參考文獻

[1] E. T. Lin, C. I. Podilchuk and E. J. Delp,“Detection of image alterations using

semi-fragile watermarks," *in Proceedings of Security and Watermarking of Multimedia Contents*, January 2000, pp. 152-163.

[2] A. Tefas and I. Pitas,"Image authentication and tamper proofing using mathematical morphology," *in Proceedings of EUSIPCO 2000*, European Signal Processing Conference, September 2000, Vol. 3, pp. 1681-1684.

[3] C. C. Chang, H. C. Hsia, and T. S Chen,"Reliable information hiding for printed images," *in Proceedings of 2000 International Symposium on Information Theory and Its Applications*, November 2000, Vol. 1, pp. 97-100.

[4] J. Huang, Y. Q. Shi, and Y. Shi, "Embedding Image Watermarks in DC Components," *IEEE Transactions on Circuits and Systems for Image Technology*, 2000, Vol. 10, No. 6, pp. 974-979.

[5] Shu Lin, Daniel J., and Costello Jr,"Error Control Coding: Fundamentals and Applications," Prentice-Hall, Englewood Cliffs, N. J., 1983.

[6] Stefan Rüping (2000): *mySVM-Manual*, University of Dortmund, Lehrstuhl Informatik 8, http://www-ai.cs.uni-dortmund.de/SOFTWARE/MYSVM。

[7] 張真誠、黃國峰及陳同孝，"電子影像技術（Electronic Imaging Techniques）"，松崗電腦圖書資料股份有限公司，2000 年 12 月。

[8] 陳同孝、張真誠及黃國峰，"數位影像處理技術"，松崗電腦圖書資料股份有限公司，2001 年 1 月。

[9] 鍾朝嵩，"相關與回歸分析"，先鋒企業管理發展中心，1982 年 3 月。

[10] 陳同孝、林泉成，"一種利用數位離散餘弦轉換及影像邊緣偵測技術設計之 列印後影像竄改防治系統"，台北科技大學－2000 年科技與管理學術研討會論文集，pp. 419-426。