植基於小波轉換及向量量化編碼之影像鑑別技術

劉江龍　婁德權　黃立中　林志麟
國防大學中正理工學院
E-mail：jlliu@ccit.edu.tw

摘要

本文提出結合離散小波轉換(Discrete Wavelet Transformation；DWT)及向量量化編碼(Vector Quantization；VQ)的影像鑑別技術。本方法首先利用離散小波轉換將影像轉換至頻率域，並萃取出鑑別及還原用的特徵值，再利用向量量化編碼壓縮特徵值，以加速後續簽章加密的速度。接收者則利用簽章內的特徵值判斷所收到的影像是否遭到竄改及復原被竄改的影像。實驗結果顯示本文所提出的方法能有效的鑑別影像是否遭到竄改，並對被竄改的區域做適度的復原。

關鍵詞：影像鑑別、離散小波轉換、向量量化編碼、數位簽章、竄改偵測、竄改還原。

1.前言

網際網路的快速發展使得數位影像可以非常便捷地透過網路進行交換。然而，電腦技術的進步也使得非法者能夠輕易的複製影像，甚至利用人類視覺系統(Human Visual System；HVS)的特性，竄改人們所看到的影像而不被察覺。因此，影像識別系統及鑑別影像是否完整的技術成為近年來非常熱門的研究領域。一般來說，影像鑑別技術被歸類為確保影像內容沒有被更改的技術，或是影像的可視重要特徵在經過非惡意的影像處理後(例如：JPEG 壓縮)仍然被保留下來。換句話說，數位影像鑑別技術的功能是確認數位影像的完整性(Integrity)。此外，當影像遭受竄改之後，也能利用數位影像鑑別技術將竄改的區域定位出來。影像鑑別技術的應用例如：醫學影像、軍事影像、新聞及政府公告。

影像鑑別技術的另一項功能在於確認影像傳送者的身份。接收者可能經由電子郵件或網路上的伺服主機下載數位影像，也因此讓惡意的第三者有機會可以竄改原始影像。所以，接收者必須確定他所收到的影像是發送者的原始影像。我們將這種功能稱為影像合法性(Legitimacy)的鑑別。

為了達到鑑別影像的「完整性」與「合法性」，目前已有許多的影像鑑別方法被提出。根據儲存鑑別資料的方式，影像鑑別技術可概分為兩類：植基於標記技術(Labeling-based Techniques)[9]與植基於浮水印技術(Watermarking-based Techniques)[15]。這兩類方法的主要不同在於植基於標記技術的方法是將鑑別資料另外存成一個檔案，而植基於浮水印技術的方法則是將鑑別資料嵌入原圖中。兩個方法各有其應用的領域，本文所採用的方法則為植基於標記的影像鑑別技術。

近幾年來，越來越多的研究學者紛紛投入影像鑑別技術的研究領域中，許多相關的影像鑑別技術也陸續被提出。一個成功的影像鑑別技術，在設計過程中，需依循著不同應用與需求來考量整體架構。一般而言，影像鑑別技術具備下列特性[1]：

(1)有效性(Effectiveness)：當一張影像遭受到惡意地竄改，一個成功的影像鑑別技術必須有效地指出遭受竄改的位置。

(2)還原能力(Recoverability)：針對一張遭受竄改的影像，不需參考原始影像，即能從簽章中取出還原所須的資訊，並針對遭受竄改的影像進行適度的還原；亦即一個好的影像鑑別技術，必須具有將內容還原的能力。

(3)辨別性(Differentiation)：一個好的影像鑑別技術必須區分出這張影像是善意的調整，還是遭受到惡意的竄改。亦即不能將善意的影像調整當作惡意的竄改，也不能將惡意的竄改當作是善意的調整。

(4)安全性(Security)：一個好的影像鑑別技術必需結合一個好的加密技術，以保護萃取出的特徵值，進而能夠驗證影像的完整性。

(5)負載(Capacity)：負載就是影像特徵值的最大資料量。影像特徵值的大小直接影響後續的數位簽章加密的速度，數位簽章必須在理想的時間內完成，如果須要加密的影像特徵值太大，將會導致花費太多時間在數位簽章的製作上。

本文結合離散小波轉換及向量量化編碼提出同時具備有效性、還原能力、安全性、辨別性等特性的影像鑑別技術。

為完整說明本文提出之方法(以下簡稱本方法)，本文其餘各節安排如下：第 2 節介紹與本方法相關之技術，包括：Haar 離散小波技術及向量量化編碼法；第 3 節詳細說明本文提出的方法；第 4 節以實驗證明本方法之有效性及實用性；第 5 節為本文之總結。

2.相關技術探討

本文提出的方法是將原圖進行三階離散小波轉換以萃取影像特徵值，因小波係數保有的空間域特性，我們使用向量量化編碼法來壓縮特徵值，並結合數位簽章技術，提供良好的安全機制。以下介紹本文提出方法的核心技術：Haar 離散小波轉換與向量量化編碼。

2.1 Haar 離散小波轉換

目前離散小波轉換方法有很多種[3,13-14]，Haar 轉換法[2]是目前最快、也最常使用的離散小波轉換方法。Haar 轉換法將空間域影像中的像素顏色值視為獨立數值，並藉由像素之間相加與相減的運算過程，求出各個頻帶的小波係數值。

在 Haar 轉換法中，相加的部分代表低頻，而相減的部分代表高頻；藉由相加相減的運算，產生重要性不同的頻帶。Haar 運算分為兩個步驟：一為水平切割，另一個則為垂直切割。水平切割是依序由左至右的方向讀取係數，將運算結果也依水平方向依序儲存。垂直切割則是由上至下的方向讀取係數，經過運算後的係數值也是依照垂直方向存放。以下以一階離散小波轉換方式為例，說明 Haar 函數的運算過程：

步驟一：水平分割程序。依序由左至右的水平方向，讀取空間域原始影像的矩陣像素值，取出相鄰兩像素進行相加與相減運算，將運算後之結果以水平方向儲存。在圖 1 中，A、B、C 及 D 分別表示為空間域影像中四點像素值；首先，取出 A 與 B 兩像素，將兩點進行相加(A+B)運算與相減(A–B)運算。接下來，取出 C 與 D 兩像素進行相加(C+D)運算與相減(C–D)運算，將運算結果儲存。相加的區域就是空間域影像的低頻區，以符號 L 表示，相減的區域則是空間域影像的高頻區，以符號 H 表示。

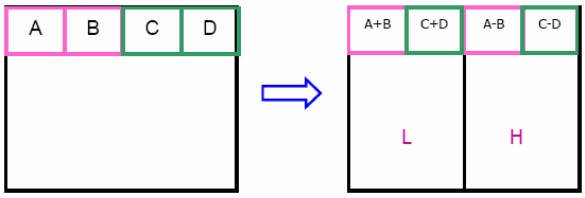


圖 1 水平切割示意圖

步驟二：垂直分割程序。將水平分割後的結果依照由上而下的垂直方向，取出係數值進行再一次相加與相減的運算，其運算後的結果也分別以垂直方向儲存。圖 2 中，A、B、C 及 D 為水平分割後所產生的係數值，依照垂直方向分別取出 A 與 B 兩係數，並進行相加(A+B)、相減(A–B)運算，將其結果儲存在左邊陣列之中。係數值相加後的結果為低頻中的低頻，以符號 LL 表示，相減後的係數值是低頻中的高頻，以符號 LH 表示。接下來，取出 C 與 D 兩係數再度進行相加與相減運算，相加後的係數值為高頻中的低頻，以符號 HL 表示，相減後的係數值為高頻中的高頻，以符號 HH 表示。

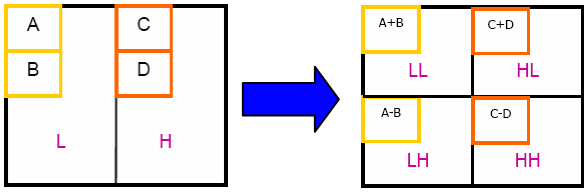


圖 2 垂直切割示意圖

水平分割與垂直分割完成後，所得到的結果就是第一階離散小波轉換後的矩陣，符號 LL、HL、LH 及 HH 區塊稱為頻帶，其中以 LL 頻帶為頻率域影像中最重要的區域，所以四個頻帶中以 LL 頻帶的小波係數對影像的重建最為重要。

2.2 向量量化編碼

向量量化編碼技術是一個非常有效率的壓縮方法[4-10]。在開始進行向量量化編碼之前，我們必須先建立一本編碼書。

最常使用來訓練編碼書的方法是 1980 年由 Linde, Buzo 及 Gray 三人所提出的 LBG 演算法[12]。以下將介紹 LBG 演算法。首先，我們先給定二個集合分別為訓練區塊的集合 $B_1, B_2, ..., B_n$ 及初始編碼字的集合 $C_1, C_2, ..., C_m$ $(n > m)$。然後，訓練區塊將被初始編碼字分成 m 個群。藉由計算每一個訓練區塊與每一個初始編碼字(Codeword)的歐幾里德距離，訓練區塊將被分別歸類到與其最接近的初始編碼字。將所有的訓練區塊分配到最接近的群後，LBG 演算法會計算每一個群裡面的區塊平均值，並以此平均值取代原先的編碼字。LBG 演算法會反覆的運算直到差距小於預先設定的值才會停止。由於 LBG 演算法能夠為訓練區塊找到最佳的編碼書，因此，將編碼書使用在向量量化壓縮時，不會產生過大的失真。

在進行數位影像編碼前，首先要先將大小 $N \times N$ 的原始影像 I 切割為數個互不重疊且大小相同的影像區塊 $B_1, B_2, ..., B_r$，每個區塊的大小均為 $K \times K$，總區塊數 $r = N \times N / K \times K$。接著，分別計算每一個區塊 B_i 與編碼字的歐幾里德距離，以找出 B_i 與編碼書裡最接近的編碼字 V_i。再來使用 V_i 的索引值 P_i 來代替 B_i。最後，將所有的影像區塊 $B_1, B_2, ..., B_r$ 都轉換成索引值 $P_1, P_2, ...P_r$。經由向量量化壓縮，影像 I 被轉換成索引值 $P_1, P_2, ...P_r$ 的集合。所以，向量量化壓縮可以有很大的壓縮率。其壓縮率等於 $1 / K \times K$ 乘以索引值的位元數。

每一個壓縮資料的索引值經由編碼書找到相

對應的編碼字。然後，組合這些相對應的編碼字即可產生恢復影像。

3.植基於小波轉換及向量量化編碼之影像鑑別技術

本文提出的方法首先將影像進行離散小波轉換，從中萃取出重要的特徵值，再利用向量量化壓縮萃取出之特徵值，得到一索引值，並利用發送者的私密金鑰對此索引值加密，得到一加密簽章，最後將原始影像與簽章一起傳送給接收者。如果傳送過程中，影像遭受竄改或破壞，則接收者可以透過簽章的驗證程序定位出被竄改的區域，並對被竄改區域做適度的復原。細節分述於以下各小節。

3.1 簽章產生

將原圖經過三階離散小波轉換(如圖 3 所示)，取出 LL3 頻帶的係數做為偵測用的特徵值，據以判斷影像是否遭受惡意竄改，另取出 LL1 頻帶的係數做為影像還原的特徵值。

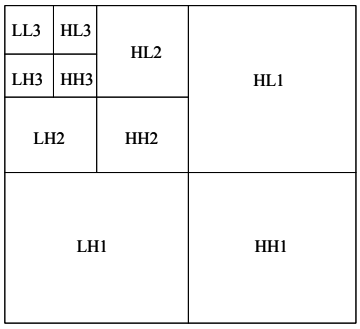


圖 3 三階離散小波轉換示意圖

針對 LL3 頻帶係數部份，首先選擇 α 維度(dimension)的編碼字(Codeword)及 m 長度的編碼書(Codebook)，然後利用 LBG 演算法，得到 LL3 頻帶係數的編碼書 $\Omega_d = \{C_1^d, C_2^d, ..., C_m^d\}$。以相同的方法，選擇 β 維度的編碼字及 n 長度的編碼書，得到 LL1 頻帶係數的編碼書 $\Omega_r = \{C_1^r, C_2^r, ..., C_n^r\}$，其中 C_i^d 及 C_j^r 分別為 Ω_d 及 Ω_r 的編碼字，分別表示為 α 維度向量 $C_i^d = (C_{i1}^d, C_{i2}^d, ..., C_{i\alpha}^d)$ 及 β 維度向量 $C_j^r = (C_{j1}^r, C_{j2}^r, ..., C_{j\beta}^r)$。決定了編碼書 Ω_d、Ω_r 的長度及編碼字 C_i^d、C_j^r 的維度後，反覆使用 LBG 演算法對大量的圖檔訓練，據以得到我們所需要的編碼書。

假設發送者和接收者擁有經過相同訓練後的編碼書，發送者便可利用編碼書對原圖做向量量化編碼，得到量化後的 LL3 及 LL1 頻帶係數值(分別以 O_{LL3} 與 O_{LL1} 表示)，然後，萃取出索引值 C_i^d、C_j^r 的集合，以達到壓縮 LL3 及 LL1 頻帶係數的目的，最後，使用發送者的私密金鑰對索引值加密，即可得到所要之數位簽章。之後，數位簽章可連同欲傳輸的影像傳送給收方，以作為竄改偵測與還原之用。

3.2 影像竄改偵測與還原

首先利用離散小波轉換萃取出待測影像的 LL3 及 LL1 頻帶係數值，將萃取出的 LL3 及 LL1 頻帶係數值藉由編碼書進行向量量化編碼，得到量化後的 LL3 及 LL1 係數值(分別以 T_{LL3} 與 T_{LL1} 表示)；再利用發送者的公開金鑰將收到的數位簽章解密，得到索引值 C_i^d 及 C_j^r 的集合；配合編碼書及索引值 C_i^d 及 C_j^r 的集合可得到原圖 LL3 及 LL1 量化後的係數值 O_{LL3} 及 O_{LL1}。最後比較 T_{LL3} 及 O_{LL3} 以判定影像是否遭受惡意竄改。如果影像遭受竄改，則利用簽章中的 O_{LL1} 對遭受竄改的區域作適度的復原。

3.2.1 竄改偵測

本方法是利用簽章所推導出的 O_{LL3} 值作為偵測影像是否遭受竄改的依據，竄改偵測的詳細步驟如下：

(1)將待測影像 T 進行三階離散小波轉換。
(2)取出待測影像的 LL3 頻帶係數，並進行向量量化編碼，得到 T_{LL3}。
(3)由簽章取出原圖量化後 LL3 頻帶係數的索引值集合 C_i^d，並利用編碼書得到原圖量化後的 LL3 頻帶係數 O_{LL3}。
(4)以 T_{LL3} 減去 O_{LL3}，檢視相減後各區塊的數值。
(5)如果相減後該區塊數值為零，則影像未被竄改，若該區塊數值非零，則記錄其位置。
(6)將未被竄改區塊的係數更改為 0，保留遭受竄改區域的係數值。
(7)反離散小波轉換後，標示出遭受竄改區域。

3.2.2 竄改還原

利用簽章所推導出的 O_{LL1} 值，我們可將受竄改的影像做適度的還原。其步驟如下：

(1)將待測影像 T 進行一階離散小波轉換。
(2)取出簽章中原圖量化後 LL1 係數的索引值集合 C_j^r，並利用編碼書得到原圖量化後的 LL1 係數值 O_{LL1}。
(3)利用 3.3.1 節中所定位出的竄改區塊，以 O_{LL1} 係數中相對位置的區塊取代被竄改的區塊。
(4)將相對於被竄改區塊位置的 LH1、HL1 及 HH1 係數更改為零。
(5)執行反離散小波轉換，就能得到適度還原後影像。

3.3 區別惡意竄改與非惡意竄改

區別惡意破壞與非惡意破壞為影像鑑別最常碰到的問題。為了節省傳輸時間或儲存空間，失真性影像壓縮技術是我們最常使用的方式，只要犧牲一點點的影像品質，但不影響影像內容，就可以大大的減少傳輸時間及減少儲存空間，目前最常用的技術就是 JPEG 壓縮技術。雖然 JPEG 壓縮技術使影像可以更便捷的在網路交換，但是，這也令大部份的影像鑑別程式發生了誤判情形，因此，如何區別待測影像是遭受惡意攻擊或只是經過 JPEG 失真性壓縮，為目前的一大挑戰。

以頻率域的觀點來看，大部份的影像壓縮軟體都是針對圖檔的高頻部份進行壓縮，本文提出的方法是萃取圖檔的低頻部份作為判斷影像是否遭受竄改的特徵值，因此，大大的降低了誤判的機率。

另外，發送者可以在製作簽章時，先將原圖以 JPEG 壓縮技術進行壓縮，得到壓縮後圖檔 O'；再萃取壓縮圖檔 O' 經過向量量化編碼後的 LL3 頻帶係數 O'_{LL3}，並計算 O'_{LL3} 及 O_{LL3} 的均方根錯誤率(Mean-Square Error；MSE)，取其最大數作為門檻值 t，以門檻值 t 判斷影像為經過 JPEG 壓縮處理或遭到惡意竄改的攻擊。

4.實驗結果

本節將針對本文提出之影像鑑別技術設計實驗，以驗證所提出的方法可以有效且準確的定位出微小區域(大小為 3 個像素)的竄改，且對於大區域的影像竄改也可以保有良好的復原效果。此外，我們以實驗證實本論文提出的方法藉由門檻值 t 的設定，可以有效區別 JPEG 壓縮後的圖檔與惡意竄改後的圖檔。最後，藉由與其他文獻實驗結果之比較來突顯本方法的優點。

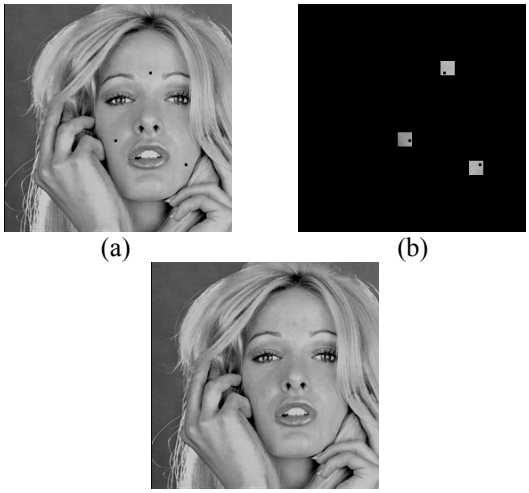
本文所使用的原始影像為 8 位元灰階影像的 Woman、F-16 等 256×256 像素圖檔 (如圖 4 所示)。此外，編碼書及編碼字的大小關係著影像鑑別時的有效性及影像復原時的回復品質，但是，編碼書和編碼字如果太大則無法發揮向量量化高壓縮率的優點。因此，本文使用的 LL3 係數編碼書其大小為 64，編碼字為 4 位元；LL1 係數編碼書其大小為 128，編碼字為 16 位元。

(a) Woman (b)F-16

圖 4 實驗用 8 位元灰階影像

4.1 小區域竄改偵測與還原

在 Woman 臉上添加 3 個像素大小的小黑點，以驗證本文提出的方法可以有效偵測出輕微的竄改並復原。圖 5(a)為遭受竄改影像(PSNR 值為 37.41dB)，圖 5(b)為竄改偵測圖，圖 5(c)為復原竄改區域後影像(PSNR 值為 54.26dB)。



(a) (b)

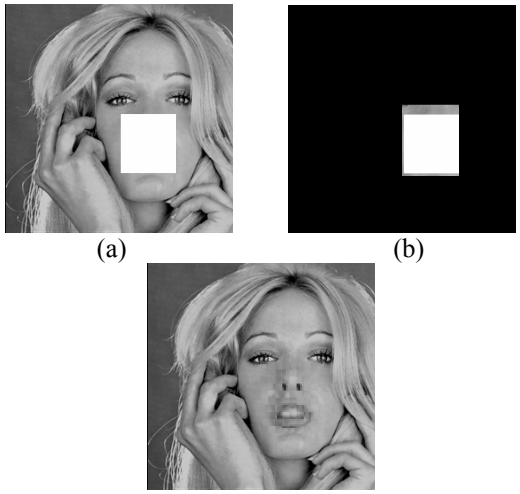
(c)

圖 5 小區域竄改偵測及還原結果

從上述實驗顯示，本文提出的方法可有效偵測出小區域的竄改，並提供良好還原效果。

4.2 大區域竄改偵測與還原

圖 6(a)為對 Woman 影像進行切割攻擊，圖 6(b)為竄改偵測圖，圖 6(c)為復原後的影像。



(a) (b)

(c)

圖 6 大區域竄改偵測及還原結果

我們另外對 F-16 影像進行大面積的竄改攻

擊，以測試本方法可適用於所有影像。表 1 為大區域影像遭受攻擊及還原後的數據。

表 1 大區域竄改之還原效能表

影像	攻擊後 PSNR(dB)	復原後 PSNR(dB)	最大 MSE 值
Woman	19.40	36.50	68486
F-16	18.86	39.77	94038

上述實驗結果顯示本文提出的方法不但可以有效定位出影像遭受竄改攻擊區域，對於大區域的影像竄改仍然可以保有非常好的還原能力(PSNR 值皆可達 36dB 以上)。

4.3 區別 JPEG 壓縮

對實驗圖像進行 JPEG 壓縮，並計算壓縮後的均方根錯誤率(MSE)。表 2 為不同的 JPEG 壓縮品質因子下的 MSE 值與 PSNR 值；接著對實驗圖像進行惡意竄改，以驗證提出方法抗 JPEG 壓縮的能力。表 3 為惡意竄改後的 MSE 值與 PSNR 值。

表 2 不同的 JPEG 壓縮品質因子下的 MSE 值與 PSNR 值

JPEG 壓縮品質因子		MSE 值	壓縮後 PSNR 值
Woman	75	0	41.61
	50	1353.9	37.18
	25	2617.5	33.86
F-16	75	0	41.62
	50	854.21	36.82
	25	4537.9	33.26

表 3 惡意竄改後的 MSE 值與 PSNR 值

實驗影像	惡意竄改後 MSE 值	惡意攻擊後 PSNR 值	復原後 PSNR 值
Woman	5698.4	37.41	54.26
F-16	9024.4	36.66	40.85

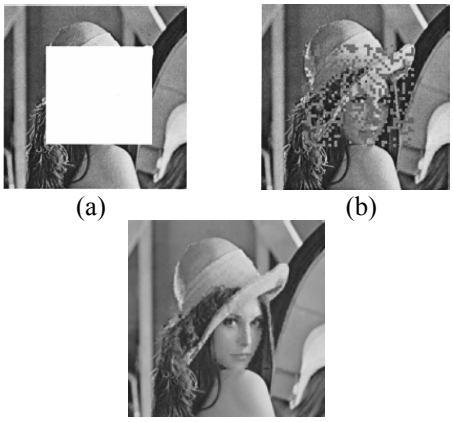
我們可由表 2 與表 3 看出，即使把 Woman 的品質因子設定在 25，其 MSE 值為 2617.5，遠小於惡意攻擊後的 MSE 值 5698.4。因此，發送者可以在傳送檔案前根據 JPEG 壓縮後的 MSE 值設定一門檻值 t，當接收者進行影像鑑別時發現最大的 MSE 值遠大於門檻值，則影像是不可信賴的，因此，接收者必須進行影像竄改定位及還原，否則，則認為影像是可信賴的。

4.4 比較與討論

在 Hung 等人[11]所提出的方法中，利用向量量化法萃取出偵測用的影像特徵值 W_d 及還原用的影像特徵值 W_r，並使用邊緣相似法(Side-Match Method)將還原用的特徵值壓縮，最後將特徵值 W_d 及 W_r 嵌入經過離散餘弦轉換後的原圖中頻係數裡，利用兩份不同用途的特徵值，鑑別出受竄改的灰階影像區域且適度的還原受破壞區域影像。本方法與 Hung 等人所提出方法之比較如下：

(1) 負載(Capacity)：負載就是影像特徵值的最大資料量。Hung 等人使用於偵測用的編碼書大小為 16，編碼字維度為 16 位元；使用於還原用的編碼書大小為 256，編碼字維度為 16 位元。若實驗影像為 512×512 像素的灰階圖像，則其負載 W_d 為 128×2^4 位元，W_r 為 128×2^7 位元。本文提出的方法 W_d 為 32×2^6 位元，W_r 為 64×2^7 位元。因此，本文提出之方法的負載較小，如果將本方法所獲得的特徵值以 Hung 等人的方法隱藏在原圖中，可以減少原圖所受到的破壞。

(2) 遭受竄改影像還原後的品質：圖 7(a)為 Lena 的臉部整個被切割後的影像，圖 7(b)為使用 Hung 等人所提出之方法鑑別與還原後的影像，圖 7(c)為使用本文所提出之方法鑑別與還原後的影像。本文所提出之方法，利用離散小波轉換後重要資訊集中在低頻的特點，只取 LL1 頻帶係數做為影像復原的特徵值，因此，雖然 W_r 的資料量比 Hung 等人所提出之方法小，卻可以有較好的影像復原品質。



(a) (b) (c)

圖 7 相同的切割攻擊下影像還原後的品質比較

5.結論

本文提出結合離散小波轉換及向量量化編碼的影像鑑別技術。本方法利用 LL3 頻帶的小波係數做為偵測用的特徵值，據以判斷影像是否遭受惡意竄改，並利用 LL1 頻帶的小波係數做為影像還原的特徵值，作為還原遭受惡意竄改的影像。與現有的方法相比，本方法可用較小的負載達到鑑別惡意竄改及修復被竄改的區域，且復原後的影像具有較佳的視覺品質。此外，透過適當門檻值的設定，本方法可有效區分 JPEG 壓縮與惡意攻擊，增加本方法的實用性。實驗結果顯示本文所提出的方法能有效鑑別惡意竄改，並提供良好的還原效果。

參考文獻

[1] 張真誠、陳同孝、黃國峰，電子影像技術，松崗電腦圖書資料股份有限公司，台北，2000。

[2] 張真誠、陳同孝、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，台北，2001。

[3] Craizer, M., Silva, E. A. B. D., and Ramos, E.-G., "Convergent Algorithms for Successive Approximation Vector Quantization with Application to Wavelet Image Compression," IEE Proceedings-Vision Image and Signal Processing, Vol. 146, No. 3, pp. 159-164, 1999.

[4] Chang, C. C., Lin, D. C., and Chen, T. S., "An Improved VQ Codebook Search Algorithm Using Principal Component Analysis," Journal of Visual Communication and Image Representation, Vol. 8, No. 1, pp. 27-37, 1997.

[5] Chen, T. S., Chang, C. C., and Hwang, M. S., "A Virtual Image Cryptosystem Based upon Vector Quantization," IEEE Transactions on Image Processing, Vol. 7, No. 10, pp. 905-910, Oct. 1998.

[6] Chung, K. L., Shen, C. H., and Chang, L. C., "A Novel SVD and VQ Based Image Hiding Scheme," Pattern Recognition Letters, Vol. 22, pp. 1051-1058, 2001.

[7] Du, W. C. and Hsu, W. J., "Adaptive Data Hiding Based on VQ Compressed Images," IEE Proceedings-Vision, Image and Signal Processing, Vol. 150, No. 4, pp. 233-238, 2003.

[8] Gersho, A. and Gray, R. M., Vector Quantization and Signal Compression, Kluwer Academic Publishers, Massachusetts, 1992.

[9] Hu, Y. C. and Chang, C. C., "A Progressive Codebook Training Algorithm for Image Vector Quantization," Proceedings of the Fifth Asia-Pacific Conference on Communications (APCC '99), Vol. 2, pp. 936-939, 1999.

[10] Hu, Y. C. and Chang, C. C., "Low Complexity Index-compressed Vector Quantization for Image Compression," IEEE Transactions on Consumer Electronics, Vol. 45, No. 1, pp. 219-224, Feb. 1999.

[11] Hung, K. L., Chang, C. C., and Chen, T. S., "A Secure DCT-based Technique for Recoverable Tamper Proofing," Optical Engineering, Vol. 40, No. 9, pp. 1950-1958, 2001.

[12] Linde, Y., Buzo, A., and Gray, R.M., "An Algorithm for Vector Quantization," IEEE Transactions on Communications, Vol. 28, pp. 84-95, Jan. 1980.

[13] Munteanu, A., Cornelis, J., Van der Auwera., G.., and Cristea, P., "Wavelet Image Compression-the Quadtree Coding Approach," IEEE Transactions on Technology in Biomedicine, Vol. 3, No. 3, pp. 176-185, 1999.

[14] Shapiro, J. M., "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," IEEE Transactions on Signal Processing, Vol. 41, No. 12, pp. 3445-3462, 1993.

[15] Walton, S., "Image Authentication for a Slippery New Age," Dr. Dobb's Journal, Vol. 20, No. 4, pp. 18-26, 1995.