植基於影像修補方法且具抵抗大量修改之影像竄改偵測及還原技術

洪國龍
朝陽科技大學資訊管理學系
e-mail：
klhung@cyut.edu.tw

陳璟慶
朝陽科技大學資訊管理學系
e-mail：
s9414614@cyut.edu.tw

劉蘭瑤
朝陽科技大學資訊管理學系
e-mail：
s9614615@cyut.edu.tw

摘要

在這篇論文中，我們提出一個基於影像修補方法且具抵抗大量修改的影像竄改偵測及還原技術。首先經由 Vector Quantization(VQ)向量量化編碼法[3]壓縮後的修補資訊與偵測資訊，複製三份索引值以最低位元置換法(LSB)[7]空間域的方式藏入於一個區塊內，並使用八個方向的內插法來修補復原資訊。透過實驗結果，我們可以發現到本篇所提出的方法在還原竄改影像後還能保有非常良好的影像品質及復原能力。

關鍵詞：影像資訊隱藏、竄改偵測及還原、向量量化編碼法

Abstract

In this paper, a scheme based on image inpainting technique is proposed to resist the massive modification for image tamper detection and recovery. First, the recovery and detection information is compressed and embedded into a block via Vector Quantization (VQ) encoding. Then, the least significant bit (LSB) technique with spatial domain is used to embed three copies of into a block. Next, an interpolation technique with eight direction is employed to inpaint the recovered information. Experimental results show that the proposed scheme is effective and achieves good recovery image quality.

Keywords: information hiding, tamper detection and recovery, vector quantization encoding

1. 前言

在網路的快速發展以及資料數位化的趨勢下，數位資訊徹底顛覆了人類資訊取得的方式，資訊的取得變的相當容易。數位化的圖像與資料可以透過網際網路快速的傳遞和交流，因此任何人可以輕易取得他人的創作。

數位影像有著容易修改的特性，目前一般普遍的影像編輯軟體，如 PhotoShop、PhotoImpact，這些編輯軟體可以輕易的修改影像不留痕跡，使得這些數位影像不具有公信力。所以惡意竄改者未經原創者的同意下進行複製與修改，影響到原創作者的權益。

為了數位影像的信賴度及提升數位影像的公信力，影像偵測竄改技術已被重視且被廣泛的討論，直到目前已有許多相關研究被提出。茲列舉如下：

最早提出影像竄改偵測技術的是S. Walton [11]，這個方法要先計算一張影像所有像素的前 7 個檢查和(checksum)，然後將這些值嵌入一個亂數隨機選取位置的最低位元置換(Least-significant-bits, LSB)中。雖然這個方法可以提供很高的竄改偵測率，由於並沒有提供任何的安全機制，竄改者可以在不改變 LSB 的前提下，巧妙的竄改這張影像；且這個方法不具有分辨惡意竄改或無心的影像調整的能力。

R. B. Wolfgan and E. J. Delp [10]提出利用易碎型浮水印(fragile watermark)來作影像竄改偵測。針對一個特定影像區塊定義了一個根基在 m 序列及影像內積的非二元統計，用來判段影像區塊被竄改的程度。Wolfgran 和 Delp 提出的這個方法已具有分辨惡意竄改或無心的影像調整的能力。但是最大的缺點是浮水印藏在 LSB，竄改者仍可在不改變 LSB 的情況下，對這張影像進行竄改。

由於空間域(spatial domain)影像處理技術在遭受影像處理攻擊的抵抗能力不佳，所以目前影像竄改技術多以頻率域(frequency domain)進行研究。頻率域最主要的特性，就是可以利用少數係數來表示影像中大部分的特徵資訊，大大減少資訊量。在頻率域上的方法，最常使用的方法是離散餘弦轉換(Discrete Cosine Transformation, DCT)及離散小波轉換(Discrete

Wavelet Transformation, DWT)這兩種方法。

針對已內容為主的影像，M. Schneider and S.-F. Chang [6]以離散餘弦轉換為基礎，提出了一個影像驗證技術。這個方法主要是計算竄改影像特徵值與原始影像特徵值的相似度，進行竄改偵測。在這個方法中，影像雖然遭受影像調整，竄改部位仍可以被偵測出來，但是無法將竄改部位還原。

上面的研究，雖可以指出影像遭受到竄改部位，卻沒有探討影像被竄改後的還原能力。由於數位影像具有容易修改的特性，使得一些特殊文件如遺囑的數位型式，因無法確定是否遭受篡改，在法律上並不能成為有效證據。由於這些特殊文件的原始內容非常重要，所以一個好的解決方法必須能對被竄改的部位進行復原的動作。為了增加數位影像的信賴度，一些影像竄改還原的相關研究已被提出，茲列舉如下：

Lin et al.[4]於 2005 年中提出偵測與修補的方法，說明利用環形曲面 Torus 的原理[8][9]，提供該環形曲面的圓環半徑（Major Radius）以及該環的大小（Minor Radius），為影像的金鑰及總共切割區塊的數量，將偵測及修補的資訊以最低位元置換法(LSB)，最後二個位元嵌入於已打散的 4x4 不重複區塊中。而當影像受到惡意的竄改時，便將嵌入的偵測資訊取出做比對後，便取得受到損毀 2x2 區塊的位置，此次計算為偵測錯誤區塊的第一階段。而第二階段將區塊分割成 4x4 的區塊，在這 4x4 的區塊中，有任何一個 2x2 的區塊有錯誤，則整個 4x4 的區塊將視為損毀的區塊。第三階段以 4x4 的區塊來偵測，如果鄰近的左、左下、下、右下、右的 4x4 區塊為錯誤的區塊，中間的區塊也將視為錯誤區塊。第二、三階段的目的是為了將未被偵測到且錯誤的區塊以擴大的方法偵測出來，最後再取出修補的資訊來復原錯誤的區塊。

由於 Lin et al.會出現兩大缺點：第一，對於錯誤像素值太過於敏感，一個 4x4 區塊的單一像素值被竄改，則整個區塊將被標記為損毀的區塊；第二，如果本身的區塊與所對應的區塊皆為錯誤，將從鄰近的 3x3 區塊的平均值做復原動作。因此 Lee et al.於 2008 年提出偵測與修補的方法[5]，此方法將原始影像經過 Torus 的原理產生 look up table，再橫向切割分為上、下相等並且相互對應的區塊，以形成雙浮水印現象，將偵測及修補的資訊以最低位元置換法(LSB)，最後三個位元嵌入於已打散的 2x2 不重複區塊中。當受到竄改時，便將嵌入的偵測資訊取出做比對，而得到損毀的位置，此為偵測錯誤區塊的第一階段。第二階段在區塊附近的八個鄰近邊緣做偵測，若有四對以上標記為錯誤，中間的區塊也視為錯誤區塊。第三階段則區塊附近的八個鄰近邊緣若有五對以上標記為錯誤，則中間區塊視為錯誤區塊。第二、三階段的方法可以有效地針對大範圍的竄改區域做復原的動作。

VQ 攻擊基本的工作如下[2]：假設攻擊者，在不知的原因下，能充分地取出有嵌入浮水印的影像，其擁有相同的 key 並知道區塊使用的大小。而建立一本 VQ 編碼簿時，會使用有嵌入浮水印的區塊，攻擊者可以在未嵌入浮水印的區塊中搜尋編碼簿並找到最相配的區塊。因為浮水印的嵌入與偵測是獨立區塊的執行，驗證處理無法感覺到此類的 VQ 偽造/惡意的攻擊。

Chang et al.於2008年提出一種攻擊方法[1]，針對上節Lin et al.的方法。將修補及偵測資訊直接藏在空間域中，可以有效偵測出錯誤區塊的位置，但嵌入的資訊安全性並不高。步驟一，先將已藏入資訊的影像，以4x4的區塊取出後，再分為四個2x2的區塊。將這16個像素值的最後二個位元設為零，再算出四個2x2區塊的平均值，這些平均值將會產生出Searched Dictionary。步驟二，在已藏入浮水印的影像中，以4x4的區塊取出後，再分為四個2x2的區塊，將前兩個2x2區塊的第八個位元，以及後兩個2x2區塊的第七、八個位元取出後，便得到前面六個位元數，其後面二個位元補零後為平均值，準備與Searched Dictionary中的平均值做掃描與比對。步驟三，將Searched Dictionary與Watermarked Average的四個平均值來執行掃描比對。首先將第一個2x2區塊的平均值與Watermarked Average做比對，如果平均值相等就先標記起來，繼續往下掃描比對。而第二個2x2區塊則掃描第一個2x2所標記起來的區塊，如果平均值相等再將區塊位置標記起來，第三個與第四個2x2區塊則與第二個2x2區塊的步驟相同。最後，如果這四個區塊全部都相等，則搜尋比對出以Torus方式嵌入資訊的對應區塊中。此方法不需金鑰就可以將大部份藏入的資訊正確地截取出來並再加以竄改。

在我們提出的方法中，先將影像利用 VQ 壓縮後的資訊，以隨機不同位置的三份索引表資訊與五個 Checksum 值以 LSB 的嵌入方法一次藏入三份復原資訊與偵測資訊，當影像受到

大量的竄改攻擊時，將嵌入的復原及驗證資訊取出，再做驗證資訊的比對，得到影像竄改區塊位置，由於大量竄改影像資訊，會造成偵測不準確性，所以藉著本論文所提的不需任何資訊便可準確地偵測出錯誤區塊的方法來提高偵測率，最後利用八方向的內插法來修復壓縮後的影像資訊。接著使用三份復原影像交叉比對，便能得到大量的回復資訊，修補被大量竄改的影像資訊。

其主要目的在於如果受到大量的惡意竄改攻擊時，將嵌入的資訊取出，再驗證嵌入資訊是否正確，每一個 4x4 區塊中，都藏有三份不同區塊的索引值，如果有受到毀損也可經由其它的區塊來回復藏入的索引值。

本篇論文的內容大綱如下：我們將在第二章節提出抵抗大量修改之影像竄改偵測及還原技術；接著第三章節的實驗結果會呈現出本篇方法對於較大範圍的裁剪攻擊，將有著良好的復原能力；最後在第四章節做此篇論文的總結。

2.研究方法

2.1 影像資訊隱藏程序

本小節介紹影像如何產生出修補資訊及驗證資訊具有強韌性嵌入流程(如圖 1)及方法。第一部份為如何產生修補資訊平均值與差值，第二部份說明隨機亂數產生器的方法，最後第三部份介紹的是最低位元置換(LSB)的方法。

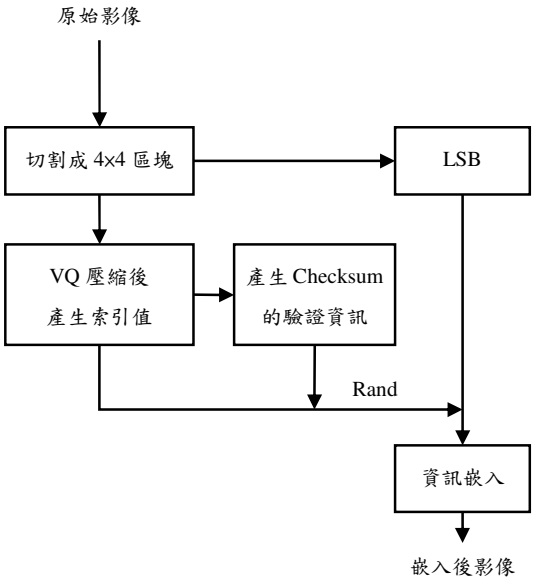


圖 1 VQ 索引值資訊及驗證資訊產生與嵌入流程

2.2 隨機亂數產生器

亂數是一個用來增強並使電子傳輸安全的基本原理；是密碼學、數位簽章、安全協定(Security Protocols)…等技術的關鍵元件，應用領域非常廣泛。一般而言，「亂數」會讓人聯想到不可預測、運氣和機會，在數學中將這些視為可計算的隨機數字。因此，亂數可以說是「在任何給定範圍的數字中，一連串有明確分散性與明確或然性的獨立數字」。

由亂數的定義可知，亂數產生器就是在有限的資料集裡，提供一連串平均分佈、不可預測、且獨立的位元資料，基於電腦的安全性，亂數產生器非常的重要。而安全性的關鍵在於一把金鑰(Key)的產生，金鑰的產生也依賴著亂數產生器，可使應用的研究具有認證性、安全性與完整性。

本篇方法隨機亂數主要目的為了將索引值打散藏入不同的影像區塊中。

2.3 三份索引值資訊嵌入方法與 Checksum 資訊的產生

最低位元置換法(LSB)[7]，將資訊隱藏於影像像素(pixel)中最後幾個位元為資料隱藏技術方法之一。灰階影像每一個影像像素是用 8 個位元 0~255 來表示，此 8 個位元中，當後面的位元遭到變更時，其數值的改變對影像的變化是非常小，所以將機密資訊嵌入於原始的影像像素後面幾個位元中的機密資訊。而原始影像也稱為掩護影像(Cover Image)，所產生嵌入機密資訊後的影像，即偽裝影像(Stego Image)，經由人眼視覺並不容易被察覺有隱藏資訊。所以，最低位元嵌入技術可以說是一個最簡易、對掩護影像影響最小的資訊隱藏技術。

而本篇方法是將 VQ 壓縮產生出來的編碼簿大小為 512 的索引值，維度大小為 128x128，使用隨機亂數產生器取出隨機三個索引值共 27 個位元，再以這三組索引值計算 5 個位元檢查和(Checksum)，產生一組驗證值(如公式 1)，在嵌入資料時一併將 5 個位元 Checksum 嵌入。取出嵌入三份索引值資訊後再計算一次，如果計算嵌入的三份索引值的 Checksum 與嵌入的 Checksum 相等，就證明傳送的資料正確，嵌入的機密資訊可以進行檢查的一種簡單方法，復原資訊及檢查和嵌入資訊流程(如圖 2)。

$$Checksum = \left(\sum_{i=1}^{3} index(i) + 16 \right) \% \ 32 \qquad (1)$$

而嵌入的方法以最低位元置換法(LSB)[7]在原始影像中取出 4x4 的影像區塊共 16 個像素，再以 LSB 的方法藏入最後 2 個位元，總共可以藏入 32 個位元，剛好可以藏入三份的隨機索引值的資料以及 5 個位元的檢查和(Checksum)，嵌入方法(如圖 3)。

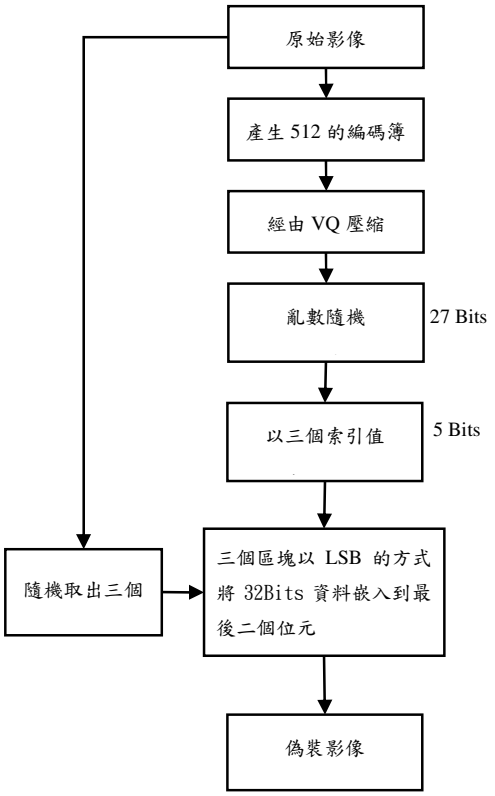
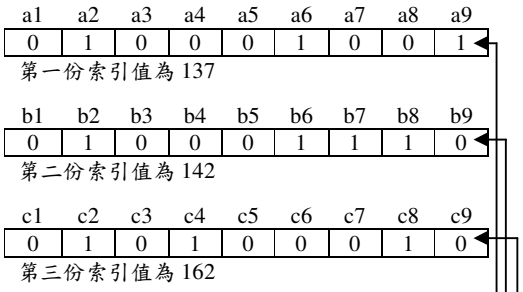


圖 2 復原資訊及檢查和嵌入資訊流程圖

2.4 竄改偵測與還原

在進行影像的竄改偵測時，需要良好的偵測能力，才能讓修補的演算法發揮出來，提高影像修補的品質，影像竄改偵測與還原的流程(如圖 4)。

第一先判斷是否受到竄改的攻擊，然後再確定萃取出來的驗證資訊與計算後的驗證資訊及索引值是否相等，藉著驗證資訊與索引值的雙重比對，可以讓錯誤偵測更為準確。



Bit	8	7	6	5	4	3	2	1
D1							a1	a2
D2							a3	a4
D3							a5	a6
D4							a7	a8
D5							a9	b1
D6							b2	b3
D7							b4	b5
D8							b6	b7
D9							b8	b9
D10							c1	c2
D11							c3	c4
D12							c5	c6
D13							c7	c8
D14							c9	Check-sum1
D15							Check-sum2	Check-sum3
D16							Check-sum4	Check-sum5

圖 3 三份索引值與檢查和以 LSB 嵌入資訊

接著在二元影像的遮罩上再使用高斯低通濾波器，而高斯低通濾波器具有錯誤遮罩擴大的特性，藉此來提高偵測的正確性，以上方法主要目的是為了更準確的偵測出錯誤的區塊位置(如公式 2)。

$$G(u,v) = \frac{1}{2\pi\sigma^2} e^{-(u^2+v^2)/(2\sigma^2)} \qquad (2)$$

σ 是常態分佈的標準偏差。在二維空間中，每個像素值都是周圍相鄰像素值的加權平均。原始像素的值有最大的高斯分佈值，所以有最大的權重，相鄰像素隨著距離原始像素越來越遠，其權重也越來越小。因為高斯模糊有很好的特性，如沒有明顯的邊界，這樣就不會在濾波影像中形成影響，進行模糊處理比其它的均衡模糊濾波器更能夠保留邊緣的效果。

影像修補便不使用這些錯誤區塊位置的復原資訊進行還原，而是將復原的索引值資訊經過隨機亂數的轉換後與錯誤區塊位置合併後，由於錯誤的區塊經由隨機亂數打散後，平均分佈在影像中，再以八個方向的空間域內影

像插修補的方式復原進而達到影像的完整性。

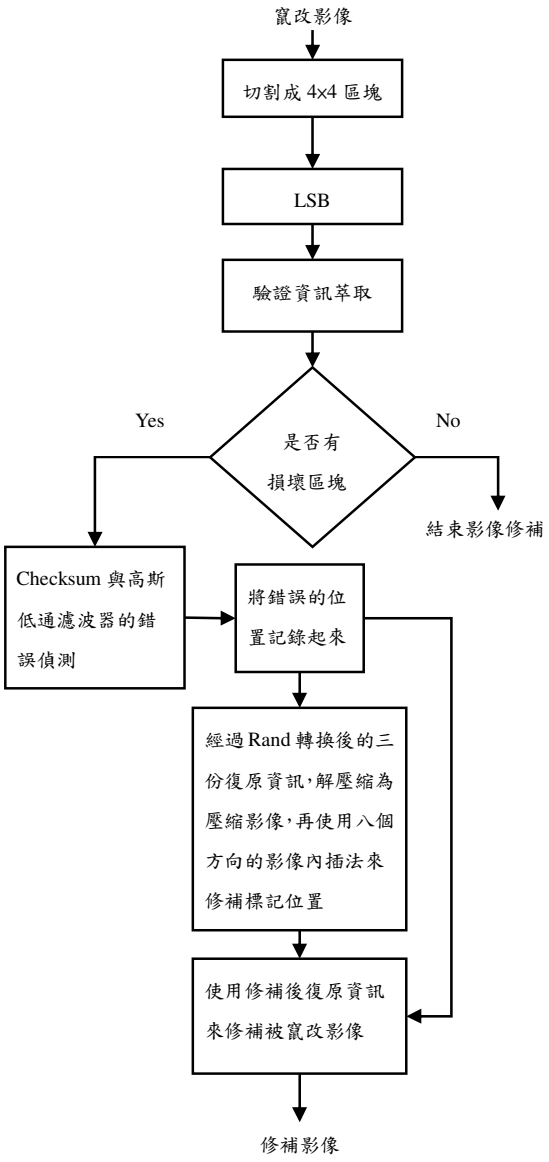


圖 4 影像竄改偵測與還原流程圖

在進行影像的竄改偵測時，先判斷是否受到竄改的攻擊，首先確定萃取出來的驗證資訊與計算後的驗證資訊是否相等，由於有三份驗證資訊與索引值，驗證資訊時會出現以下三種可能：

Case1： 如果萃取出來的三份驗證資訊為正確的，將三份索引值再做一次比對，而比對有錯，取索引值相同的二份為正確索引值，如果索引值都不相等則標記為錯誤。

Case2： 如果萃取出來二份驗證資訊為正確驗證資訊，另一份為錯誤的驗證，再來比對驗證資料正確的二份索引值，如果二份索引值不相等則標記為錯誤的。

Case3： 如果只有一份驗證資訊為正確的，則以驗證資訊對的那份索引值為正確索引值。

Case4： 如果都是錯誤的，將錯誤區塊的位置標記起來。

本研究可以藉著驗證資訊與索引值的雙重比對，能讓錯誤偵測更為準確，但還是有極小的機率有可能驗證資訊錯誤，而我們在錯誤偵測的遮罩上使用高斯低通濾波器。

高斯低通濾波器主要是用來降低雜訊及模糊，由於高斯低通濾波器的計算為每一個像素值與周圍相鄰像素值的加權平均，所以較大的標準差值會產生較平的曲線、擴散模糊的效果，較小的標準差則產生較尖的曲線。

使用高斯低通濾波器具有錯誤擴大的效果，將未偵測到的錯誤點利用濾波器的特性，來提高偵測的正確性(如圖 5)，圖 5 的(a)為被竄改的影像，而圖 5(b)為錯誤偵測的遮罩，白色為偵測出錯誤位置，圖 5(c)是應用高斯低通濾波器的結果，以上方法主要目的是為了更準確的偵測出錯誤的區塊位置。

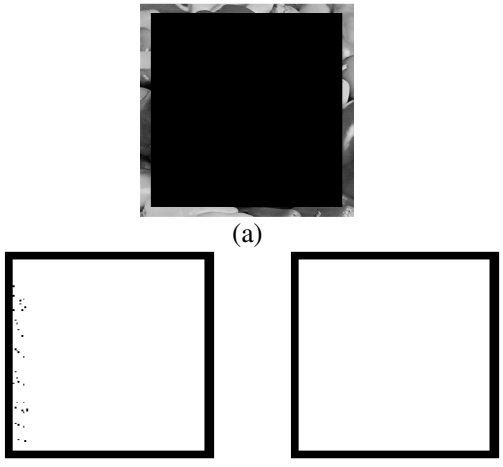


圖 5 經由高斯低通濾波器擴散模糊的特性，提高偵測的正確性

2.5 八個方向內插影像修補

影像修補便不使用這些錯誤區塊位置的復原資訊進行還原，而是將復原的索引值資訊經過隨機亂數的轉換後與錯誤區塊位置合併後，由於錯誤的區塊經由隨機亂數打散後，平

均分佈在影像中，再以損壞影像點的八個方向的空間域內影像插修補的方式復原(如圖 6)，進而達到影像的完整性(如公式 3 與 4)。

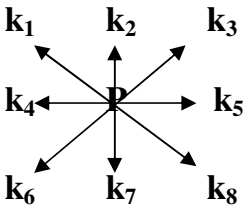


圖 6 損壞影像點的八個方向

$$Wk = 1/d(k) \quad (3)$$

$$P = \sum_{k=1}^{8} P_{(k)} \times W_{(k)} / \sum_{k=1}^{8} W_k \quad (4)$$

3.實驗結果

在實驗中，本研究使用 Windows XP 的電腦來進行實驗，使用的影像處理軟體為 PhotoImpact X3，以及 512x512 的 Lena 灰階影像進行實驗，竄改的方式為大量的黑色區塊的竄改攻擊，藉由嵌入三份浮水印的資訊，來進行錯誤偵測及修補還原影像。

3.1 還原能力分析

本實驗主要是針對影像大量竄改的偵測與還原所進行的實驗，以 2.4%、8.01%、9.7%、25%、34%、40.1%、50%、61%、65%、70%、75%、80%、85%、90%為竄改的百分比再與 Lin et al.[4]及 Lee et al.[5]二個方法做比較(如表 1)。

雖然大量竄改還原後的影像與原始影像相較之下，復原影像呈現有些模糊且閃爍現象，經由大量竄改攻擊復原影像後，由於復原資訊會跟著受到竄改而被破壞，所以修補的影像其完整性還是有限的，但影像輪廓部位大致上都還可以被識別出來，圖 7 到圖 10 顯示 Lena 影像在不同比例(60%、70%,、80%及 90%)的裁切下的實驗結果，圖 11 到圖 13 為 Pepper 影像在不同位置下裁切 50%的實驗結果。由實驗證明本研究對於大量影像竄改後復原的數據表現非常不錯。

表 1 大量竄改後修補影像實驗結果

Tam-perd %	Loca-tion	Lin et al. (dB)	Lee et al.(dB)	Proposed (dB)
2.4%	Center	39.96	39.48	40.9879
8.01%	Corner	42.32	41.42	38.2332
9.7%	Center	36.24	35.17	37.6743
25%	Top	31.60	33.45	36.0707
34%	Center	27.37	33.01	36.5834
40.1%	Center	23.97	27.97	31.48
61%	Center	19.47	25.20	27.8597
65%	Center	-	24.57	27.128
70%	Center	-	24.16	26.0833
75%	Center	-	23.43	24.6211
80%	Center	-	22.55	23.3233
85%	Center	-	21.28	21.8753
90%	Center	-	19.86	19.4324

4.結論

本篇研究主要是基於影像修補方法且具抵抗大量竄改的影像竄改偵測及還原技術，其方法是將影像經由 VQ 壓縮後，於影像區塊中將三份索引值以 LSB 空間域的方式嵌入，利用變異數的分析方法來偵測錯誤區塊位置，使用八個方向的內插法來修補復原資訊。由實驗可知，最後還原竄改影像後還能夠保有非常良好的影像品質。

參考文獻

[1] Chang, C. C., Fan, Y. H. and Tai, W. L., "Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery," ***Pattern Recognition***, Vol. 41, No. 2, pp. 654-661, 2008.

[2] Hasan, Y. M. Y. and Hassan, A. M., " Fragile blockwise image authentication thwarting vector quantization attack," ***Signal Processing and Information Technology. Proceeding of IEEE International Symposium***, pp. 530-533, 2004.

[3] Linde, Y., Buzo, A. and Gray, R. M., "An algorithm for vector quantizer design," ***IEEE Transactions on Communications***, Vol. 28, pp. 84-95, 1980.

[4] Lin, P. L., Hsieh, C. K. and Huang, P. W., "A hierarchical digital watermarking method for image tamper detection and

recovery," ***Pattern Recognition***, Vol. 38, No. 12, pp. 2519-2529, 2005.

[5] Lee, T. Y. and Lin, S. D., "Dual watermark for image tamper detection and recovery," ***Pattern Recognition***, No. 11, pp. 3497-3506, 2008.

[6] Schneider, M. and Chang, S. F., "A robust content based digital signature for image authentication," ***Proceeding of IEEE International Conference on Image Processing***, pp. 227-230, 1996.

[7] Schyndel, R. G., Tirkel, A. Z. and Osborne, C. F., "A digital watermark," ***Proceeding of IEEE International Conference on Image Processing***, Vol. 2, pp. 86-92, 1994.

[8] Voyatzis, G. and Pitas, I., "Chaotic mixing of digital images and applications to watermarking," ***Proceeding of European Conference on Multimedia Applications***, Vol. 2, pp. 687-695, 1996.

[9] Voyatzis, G. and Pitas, I., "Applications of toral automorphisms in image watermarking," ***IEEE International Conference on Image Processing***, Vol. 1, pp. 237-240, 1996.

[10] Wolfgan, R. B. and Delp, E. J., "A watermark for digital image," ***Proceeding of IEEE International Conference on Image Processing***, pp. 219-222, 1996.

[11] Walton, S., "Image authentication for a slippery new age," ***Dr. Dobb's Journal***, Vol. 20, pp. 18-26, 1995.

(a) (b) (c)

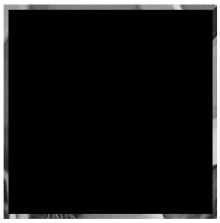
圖 7 (a) 將 Lena 裁切 60% (b) 為 Lee et al.的復原影像，PSNR 為 25.20 dB (c) 為本論文復原影像，PSNR 為 27.8597dB

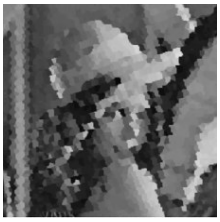
(a) (b) (c)

圖 8 (a) 將 Lena 裁切 70% (b) 為 Lee et al.的復原影像，PSNR 為 24.16 dB (c) 為本論文復原影像，PSNR 為 26.0833dB

(a) (b) (c)

圖 9 (a) 將 Lena 裁切 80% (b) 為 Lee et al.的復原影像，PSNR 為 22.55 dB (c) 為本論文復原影像，PSNR 為 23.3233dB


(a)


(b)

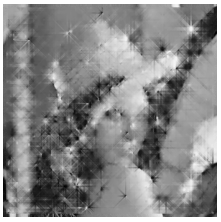

(c)

圖 10 (a) 將 Lena 裁切 90%　(b) 為 Lee et al.的復原影像，PSNR 為 19.86 dB (c) 為本論文復原影像，PSNR 為 19.4324dB


(a)


(b)


(c)

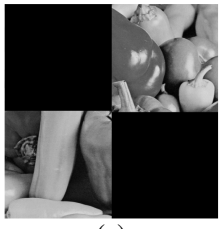
圖 11 (a) 將 Pepper 裁切 50%　(b) 為 Lee et al.復原影像，PSNR 為 27.53 dB (c) 為本論文復原影像，PSNR 為 30.2296dB


(a)


(b)


(c)

圖 12 (a) 將 Pepper 裁切 50%　(b) 為 Lee et al.復原影像，PSNR 為 26.22 dB (c) 為本論文復原影像，PSNR 為 31.0972dB


(a)


(b)

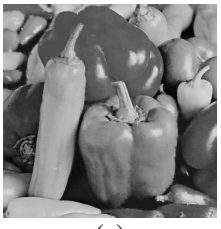

(c)

圖 13 (a) 將 Pepper 裁切 50%　(b) 為 Lee et al.復原影像，PSNR 為 29.20 dB (c) 為本論文復原影像，PSNR 為 30.4017dB