

利用小波轉換及向量化編碼法之影像隱藏技術

歐陽彥杰 黃育銓

國立中興大學電機工程學系

ycouyang@dragon.nchu.edu.tw

ychuang@mail.nchu.edu.tw

摘要

本文主要探討三種大小相同之灰階影像，機密影像 (Secret Image)、掩護影像 (Cover-Image)、及偽裝影像 (Stego-Image)。本文主要目的是希望能夠將一張機密影像隱藏至一張掩護影像後產生一張所謂偽裝影像，偽裝影像與掩護影像幾近相同，因此機密影像於網路上傳遞將不易被察覺甚至破壞。即使，一旦掩護影像被有心人士竄改、壓縮、或裁切破壞等，依據本文之技術仍可以取出機密影像。在我們所提出之資料隱藏 (Data-hiding) 技術裏，首先為了提高隱藏的資料量，機密影像會先經過 PNN、LBG、及編碼簿 (Codebook) 排序等向量化編碼 (Vector Quantization) 方法做資料壓縮。接著，為了增強抗壓縮之強韌性，掩護影像會先經過三階之離散小波轉換 (Discrete Wavelet Transform) 後，再將索引值隱藏在小波係數裏。最後，再經由反離散小波轉換 (Inverse Discrete Wavelet Transform) 後產生一張具有強韌性的偽裝影像。我們所重建的機密影像當 JPEG 壓縮品質在百分之十五以下的壓縮率，其影像品質完全不受影響，甚至在百分之五十的壓縮率，其影像仍可清晰辨識。

關鍵詞：資料隱藏、向量化編碼法、離散小波轉換、最低位元法。

Abstract

This work primarily explores three grey-level images of the same size 256×256 pixels, the secret image, the cover-image, and the stego-image. We embed a secret image into a cover-image to constitute a so-called stego-image such that the stego-image is visually indistinguishable from the original cover-image. Hence, the interceptors will not notice the existence of secret data in the stego-image. Furthermore, through our proposed data hiding scheme, the secret image still can be extracted from the stego-image even when the stego-image was attached or modified by popular image processing techniques, such as cropping and image compression.

In our proposed scheme, first, in order to increase the hiding capacity, the secret image was compressed by those techniques of vector quantization. To enhance the robust property JPEG against compression attack, the indices were embedded into the lower band through three-level discrete wavelet transform. Finally, a robust stego-image can be retrieved through the processing of inverse discrete wavelet transform. The experimental results. Show that the reconstructed

secret image can keep its original quality against JPEG compression at the compression ratio of 11% and is still be recognizable at the compression ratio of 50%.

Keywords: Data Hiding, Vector Quantization, Discrete Wavelet Transform, Least Significant Bit.

1. 前言

影像隱藏 (Image Hiding) [2] [4] [8] [9] [11] [12] [14] 的相關技術可以防止數位影像被不當竄改或破壞。當數位影像在網路上傳遞時，可以在數位影像中嵌入認證資訊來確保作者的著作權，而這一領域稱之為影像隱藏技術。

影像還原技術亦是影像隱藏技術中的一環，其主要目的就是偵測與還原所需的索引值，透過索引值重建機密影像。因此，影像還原最主要的目的，便是將已遭受竄改或破壞的數位影像還原。藉由從已被竄改或破壞的影像中取出重要的索引值得以有效還原影像，除了保持掩護影像的完整性外，進一步確保原始創作者的智慧財產權。

2. 文獻探討

2.1 資料隱藏

隱藏訊息的其中一種方式是「資料隱藏」 (Steganography)，其字面意義是「遮蔽所寫的字」，最早可回溯到古希臘時代。資料隱藏就是幾千年來把訊息隱藏在圖畫或文字之中。這門古老的科學，如今已經應用在現代通訊系統上，變成傳送訊息而不讓人察覺的一種非常有效的方式。

然而，現今資料隱藏的模式，包括把機密訊息隱藏在聲音檔案或影像之中。如果要在一個數位檔案隱藏機密訊息，通常會把機密的資訊弄亂，混進影像或聲音檔案的較不重要的位元內之中，而這種微小的變化是無法透過人類的眼睛或耳朵偵測出，以圖形為例在一張 JPEG 影像中改變幾個像素的位元組看起來並無任何異樣；所以一般人幾乎無法得知在數位影像中隱藏著重要的訊息。而這些數位影像只有利用特定的技術才能解開。否則，這些機密訊息是不可能看見。

2.2 效能評估

評估藏入影像後的影像品質，是以兩張影像之間的影像訊號雜訊比 (Peak Signal to Noise Ratios, PSNR) [7] 來表示，其表示式 (1) 如下所示：

$$PSNR = 10 \log_{10} \frac{x_{peak}^2}{MSE} \dots\dots\dots (1)$$

而公式 (1) 中的 MSE (Mean Square Error) 之定義如下列公式 (2) 所示：

$$MSE = \left(\frac{1}{M \times N} \right) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x_{ij} - x'_{ij})^2 \dots\dots\dots (2)$$

PSNR 的單位為 dB, M 和 N 分別代表了影像的寬度與高度, x_{ij} 與 x'_{ij} 則分別代表了掩護影像與藏入浮水印後的影像在座標點 (i, j) 的像素值。 x_{peak}^2 是指影像單位資料所能表示的最大值。而 PSNR 值越大, 表示兩張數位影像越相似。

3. 影像隱藏及及相關技術

本論文所運用之主要相關技術為離散小波轉換 (Discrete Wavelet Transformation, DWT)、向量化編碼法 (Vector Quantization, VQ) 及最低位元法 (Least Significant Bit, LSB) 的灰階影像隱藏技術。

3.1 影像隱藏流程

影像隱藏就是將機密影像 (Secret Image) 隱藏至另外一張影像之中, 通常稱這張被用來掩護機密影像的影像稱為掩護影像 (Cover Image), 而隱藏的動作則稱為 Image Hiding。此外, 當掩護影像在經嵌入機密影像之後, 即成為一張偽裝影像 (Stego-Image), 如圖 1 至圖 3 為研究示意圖及本文研究架構圖。偽裝影像與掩護影像之間的細微差異, 是無法用肉眼分辨出來的。因此, 影像隱藏的目的, 不僅只限於保護機密影像, 不讓未經授權的第三者, 來識別與使用該機密影像, 當攻擊者擷取偽裝影像後, 其遭受破壞後的強韌性問題, 及如何兼顧到不可發覺性與嵌入的機密影像容量, 為本文所探討之議題。

3.2 離散小波函數

離散小波轉換 (Discrete Wavelet Transformation, DWT) [1] [5] [7] [10] [13] [15] 是一種將空間域 (Spatial Domain) 影像轉換成頻率域 (Frequency Domain) 影像的技術, 當一張影像經過離散小波轉換處理後會產生重要性不同的資料, 這些資料會構成高低不同之頻率。因此, 我們就可以根據這些資料的不同重要性分別做處理。

離散小波轉換之 Haar 函數 [15] 的運算大致上有兩個步驟：一為水平分割, 另一為垂直分割, 水平分割的意思是讀取係數的順序是依照水平方向由左至右來取; 儲存時也是水平方向儲存。垂直分割的意思是讀取係數的順序是垂直方向由上至下來取, 經過運算後的數值儲存方式也是依照垂直方向存放, 反覆上述步驟即可進行二階或三階的離散小波轉換, 如圖 4 所示。

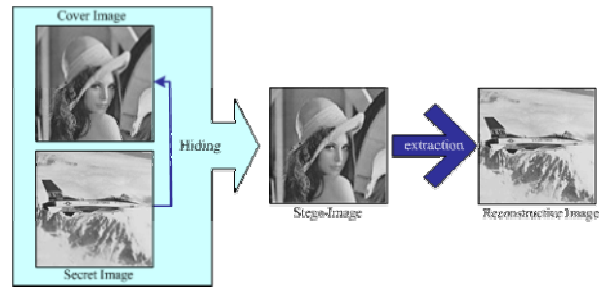


圖 1 本文研究示意圖

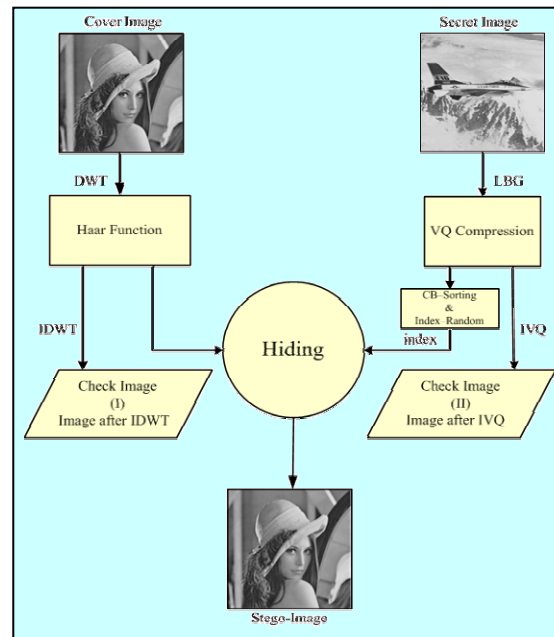


圖 2 本文研究架構—影像隱藏流程圖

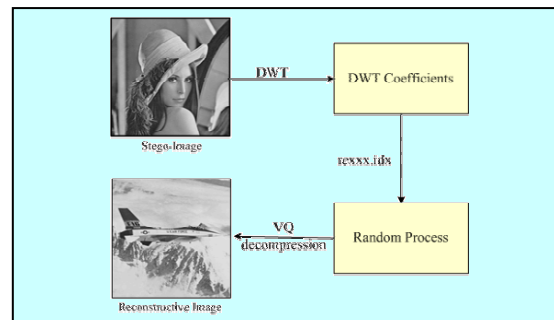


圖 3 本文研究架構—影像隱藏還原流程圖

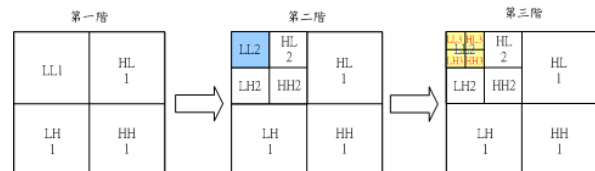


圖 4 離散小波轉換示意圖

3.3 向量化編碼法

3.3.1 原理簡介

向量化編碼法 [6] [7] [10] [11] [12] 具有失真 (Lossy) 的資料壓縮技術, 最早是由 Gray 於 1984 年所提出, 其原理由原始資料訓練出一本具代表性的編碼簿

(Codebook)，該編碼簿是由不同的向量所組成，該向量稱之為編碼字 (Codeword or Code Vector)，而編碼簿的大小與編碼字維度的大小決定了向量化壓縮結果的壓縮率。

3.3.2 向量化編碼與解碼

首先將機密影像切割成許多大小相等的區塊，每一區塊視為一個編碼向量，並假設編碼簿大小為 L 個編碼字，因此表示每個編碼字的索引值至少需要 $\log_2 L$ 個位元來表示。接下來將每一區塊依序進行向量化編碼，其編碼方式為欲編碼的區塊與編碼簿中的每一個編碼字進行向量之間距離的計算，藉此以找出與編碼區塊距離最近的編碼字，所以我們將與其距離最近的編碼字之索引值當成輸出，就可以代表此一區塊的圖像資料，如此便完成了一個區塊的編碼動作，並產生 CodeBook 及 Indices。

向量化解碼步驟就是將代表每個區塊的索引值集合，依照原來的排列順序去找尋在編碼簿當中相對應的編碼字，並以找尋到的編碼字來代表該區塊還原後的圖像資料。

3.3.3 PNN 演算法

PNN (Pairwise Nearest Neighborhood) 演算法^[7]由 W.H.Equitz 於 1989 年提出。該演算法是將每一訓練向量視為一群，然後一次一次的將兩個最接近的訓練向量合併，在每次合併後，就會重新計算新的中心點。直到達到要求的編碼簿大小為止，這些分群的中心點就形成一組編碼簿。

3.3.4 LBG 演算法

LBG 演算法^[7]是由 Linde, Buzo, Gray 三位學者於 1980 年所提出的編碼簿產生方式，稱之為 LBG 演算法，它是最常見的編碼簿訓練方式，主要是利用分群的概念，將每個訓練向量資料歸群到最接近的群，然後重新計算每群的重心以代表這一群的編碼字，再由這些代表群重心的編碼字組合而成一本編碼簿。

3.4 最低位元法

最低位元法 (Least Significant Bit, LSB)^{[3][11]}在影像隱藏領域中。最早被應用在隱藏機密影像的技術裡，其本文影像隱藏步驟如下：

Step 1: 將機密影像經 VQ 壓縮後以 8 個位元來表示索引值。

Step 2: 二階小波轉換後將此 8 個位元資料由 LSB 至 MSB 分別以 2 個位元為單位，隱藏至小波轉換之 HH2、LH2、HL2、LL2 之第 1、2 位元係數中 (如圖 5)；另三階小波轉換後將此 8 Bit 資料由 LSB 至 MSB 分別以 2 個位元為單位，隱藏至小波轉換之 HH3、LH3、HL3、LL3 之第 2、3 位元係數中 (如圖 6)。

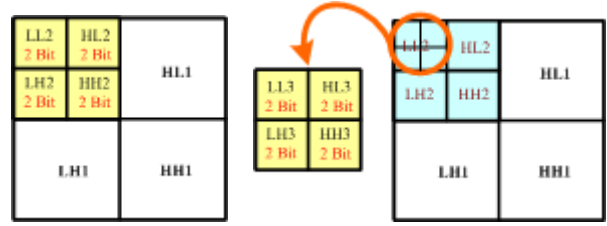


圖 5 二階位元隱藏示意圖

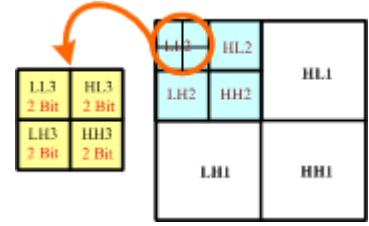


圖 6 三階位元隱藏示意圖

Step 3: 將二階小波轉換之係數最後二個位元設定為 0，並加入 Step 2 之數值；將三階小波轉換之係數最後第二及第三個位元設定為 0，並加入 Step 2 之數值。

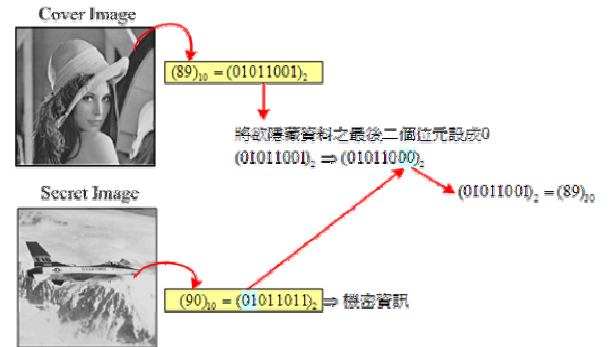
例：若原始資料 $D = 89$ ，欲隱藏 Bit 數 $N = 2$ Bit。

解：將原始料 D 依 $D = \left\lfloor \frac{D}{2^N} \right\rfloor 2^N$ 重新計算後再

將欲隱藏的資料 S 加入 D 中。

$$D = (01011001)_2 = 89_{10}, S = (01)_2$$

$$D = \left\lfloor \frac{D}{2^N} \right\rfloor 2^N = \left\lfloor \frac{89}{2^2} \right\rfloor 2^2 = 88_{10} = (01011000)_2$$



Step 4: 反離散小波轉換使小波轉換係數轉換成空間域影像，即形成為偽裝影像。

4. 實驗結果

本文主要研究為掩護影像、機密影像及偽裝影像三張相同大小的影像 (大小為 256 像素 x 256 像素)，經離散小波技術轉換及 VQ 壓縮後運用相關輔助技術以提升其抗破壞性。

4.1 實驗步驟

Step 1: 小波轉換 (Wavelet Transform)

利用離散小波函數之 Haar 函數轉換將掩護影像做二階或三階小波係數轉換，二階小波係數轉換共區分成 LL2, HL2, LH2, HH2, HL1, LH1, HH1 等七個頻段，三階小波係數轉換共區分成 LL3, HL3, LH3, HH3, HL2, LH2, HH2, HL1, LH1, HH1 等十個頻段，並將 Spatial Domain 的資訊轉為 Frequency Domain，進而刪除 Frequency Domain 的小數部分資料以去除資料在空間軸上的相關性。在此步驟將產生經小波轉換後之影像 (如圖 2 論文研究架構中之 Check Image (I))。

Step 2: VQ 壓縮 (VQ Compression)

利用 VQ 壓縮原理,透過 PNN 演算法及 LBG 演算法將機密影像 (Secret Image) 壓縮後產生 Codebook 及 Indices,隱藏至二階小波係數以 Block Size 為 16 維向量,Codebook Size 為 256;隱藏至三階小波係數以 Block Size 為 64 維向量,Codebook Size 為 256,其中將 Codebook 依灰階值 0-255 順序重新加以排列,另將索引值以亂數方式處理。

Step 3: 影像隱藏 (Image Hiding)

依據 LSB 法之方式分別隱藏 2Bit、2Bit、2Bit、2Bit 之索引值至小波係數中,使其形成偽裝影像 (Stego-Image),並計算掩護影像與偽裝影像之 PSNR 值。

Step 4: 攻擊 (破壞) 測試

我們將偽裝影像分別做 JPEG 壓縮、馬賽克、裁切等攻擊試驗,其實驗目的在探討本文研究對於資料隱藏與抗破壞之關係。

Step 5: 重建機密影像

- 5.1 經 Step 4 的實驗後,偽裝影像透過離散小波轉換之相關技術,做二階及三階的離散小波轉換,重新取回原先隱藏的索引值。
- 5.2 依離散小波轉換係數取出二階及三階的第一、二位元及第二、三位元之數值。
- 5.3 依照原先的位元分配方式重整 MSB 至 LSB 的各部分數值,產生新的索引值。
- 5.4 將重新取回的索引值結合步驟二之 Codebook 做反 VQ 壓縮轉換,重建機密影像,並計算其 PSNR 值。

4.2 機密影像經 VQ 壓縮之影像品質

我們使用 Airplane、Baboon、Eva、Goldhill、Pepper 做為實驗所需之機密影像,經 VQ 壓縮過程中使用 CodeBook Size 256,Block Size 16 之影像品質分別為 30.18 dB、25.87 dB、35.20 dB、30.64 dB、30.70 dB。

4.2.1 Codebook 經排序處理之影響

在離散小波轉換的過程中,其小波係數必須由頻率域轉回空間域影像,而此動作必須移棄小數部分,使其成為灰階影像;因此在成相及壓縮破壞的過程中即造成數值的偏移,故在重新取回索引值時就會造成誤差,此時為了減少誤差,我們以排序編碼法強化 VQ 壓縮在編碼簿區域最佳化問題,使其提升整體影像品質,因此將 Code Vector 的平均值設定為較具代表性的初始編碼簿。並將初始編碼簿依大小重新排序後,可求得更具代表性的編碼簿,以增進壓縮效能與影像品質。在本節的實驗中我們以 Airplane 做為機密影像、Lena 做為掩護影像,在經二階、三階小波轉換結合 VQ 壓縮之影像隱藏後形成偽裝影像,並以 JPEG 壓縮做為破壞性測試,其 PSNR 值提升約 2~5dB,因此三階小波轉換對於較

高的 JPEG 壓縮有顯著影響;其比較表如表 1 及表 2 所示。

表 1 二階小波轉換與排序編碼法對 JPEG 壓縮之比較表

JPEG 壓縮	未使用排序編碼法之 PSNR	使用排序編碼法之 PSNR
2 %	16.20 dB	19.07 dB
15 %	14.59 dB	18.08 dB
28 %	13.06 dB	16.54 dB
35 %	11.64 dB	14.92 dB
43 %	11.17 dB	13.61 dB

表 2 三階小波轉換與排序編碼法對 JPEG 壓縮之比較表

JPEG 壓縮	未使用排序編碼法之 PSNR	使用排序編碼法之 PSNR
2 %	30.41 dB	30.41 dB
15 %	30.41 dB	30.41 dB
28 %	27.11 dB	29.06 dB
35 %	21.21 dB	26.90 dB
43 %	17.11 dB	22.61 dB

4.2.2 Indices 經亂數處理之影響

在一張影像中,有可能某部分比另一部份有價值,於是較不重要的部分可能會被裁切,而留下部分圖形,因此偽裝影像經裁切試驗後,仍可取出機密影像,但由於小波係數轉換之緣故,會造成機密影像整塊式的破壞,若將索引值經亂數處理後,將改善此種情形,如圖 7 所示。

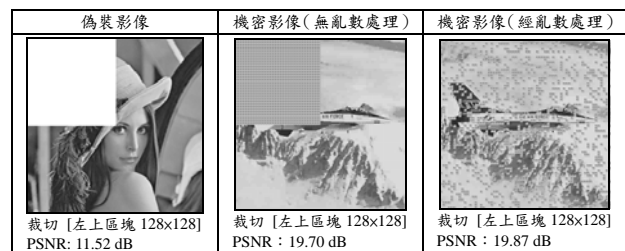


圖 1 VQ 壓縮經亂數處理之影響

4.3 偽裝影像之影像品質

本節探討掩護影像 (Lena) 經二階或三階小波轉換及機密影像 (Airplane、Baboon、Eva、Goldhill、Pepper) 隱藏後所形成的偽裝影像之影像品質。使用二階小波轉換的偽裝影像之影像品質分別為 37.83 dB、37.81 dB、37.76 dB、37.74 dB、37.79 dB;使用三階小波轉換的偽裝影像之影像品質分別為 30.57 dB、30.59 dB、30.45 dB、30.40 dB、30.45 dB。由於隱藏位置不同之關係造成三階影像品質較二階影像品質低。

4.4 破壞測試

本節以 VQ 壓縮經排序編碼法後之結果進行二階及三階小波轉換之資料隱藏實驗,其破壞實驗依 JPEG (壓縮率=2%、35%、41%、47%、50%)、馬賽克(單元格大小=2 方形)、裁切(左上區塊 128 像素x128 像素)、裁切(中間區塊 128 像素x128 像素)、裁切(右下區塊 128 像素x128 像素)等方式進行測試,其測試結果如表 3 及表 4。

表 3 Lena-Airplane 二階破壞實驗之 PSNR 值

破壞實驗	偽裝影像破壞實驗之 PSNR	經破壞實驗後取出機密影像之 PSNR (無亂數處理)	經破壞實驗後取出機密影像之 PSNR (經亂數處理)
a. JPEG [壓縮率=2%]	37.43 dB	19.12 dB	19.07 dB
b. JPEG [壓縮率=35%]	36.26 dB	15.11 dB	14.92 dB
c. JPEG [壓縮率=41%]	35.71 dB	13.52 dB	13.61 dB
d. JPEG [壓縮率=47%]	34.79 dB	12.16 dB	12.35 dB
e. 馬賽克[單元格大小=2 方形]	27.95 dB	14.73 dB	14.72 dB
f. 裁切 [左上區塊 128×128]	11.52 dB	19.70 dB	19.87 dB
g. 裁切 [中間區塊 128×128]	11.05 dB	19.29 dB	20.04 dB
h. 裁切 [右下區塊 128×128]	12.07 dB	19.92 dB	20.00 dB

表 4 Lena-Airplane 三階破壞實驗之 PSNR 值

破壞實驗	偽裝影像破壞實驗之 PSNR	經破壞實驗後取出機密影像之 PSNR (無亂數處理)	經破壞實驗後取出機密影像之 PSNR (經亂數處理)
a. JPEG [壓縮率=2%]	30.55 dB	30.41 dB	30.41 dB
b. JPEG [壓縮率=35%]	30.47 dB	26.12 dB	26.90 dB
c. JPEG [壓縮率=41%]	30.29 dB	17.70 dB	17.62 dB
d. JPEG [壓縮率=47%]	30.20 dB	16.63 dB	16.78 dB
e. 馬賽克[單元格大小=2 方形]	27.06 dB	14.14 dB	14.25 dB
f. 裁切 [左上區塊 128×128]	11.48 dB	15.63 dB	15.44 dB
g. 裁切 [中間區塊 128×128]	11.03 dB	14.09 dB	14.36 dB
h. 裁切 [右下區塊 128×128]	12.03 dB	15.83 dB	15.89 dB

4.5 離散小波轉換抵抗 JPEG 壓縮之比較

本文在二階小波轉換後之偽裝影像於 2% 的 JPEG 壓縮率下，重新取回機密影像時即有雜點產生（如圖 8），而三階小波轉換後之偽裝影像於 15% 的 JPEG 壓縮率下，仍可完整取回機密影像且無雜點產生。

經二階及三階小波轉換後對於抵抗 JPEG 壓縮可達 40%–50%，如圖 9 為三階小波轉換後經 JPEG 壓縮 50% 之重建機密影像。

而參考文獻^[12]所採用的方法，偽裝影像經 VQ 壓縮後，直接將索引值平均分配隱藏入掩護影像之 Spatial Domain 的最後一個位元中，即掩護影像未採用離散小波轉換技術轉換至 Frequency Domain，所以可以得到較佳的 PSNR 值約 54dB，但對於機密影像的抗破壞性則完全無法抵抗。



圖2 JPEG (2%)
PSNR : 19.07 dB

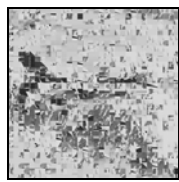


圖3 JPEG (50%)
PSNR : 16.78 dB



圖4 JPEG (82%)
PSNR : 14.04 dB

此外，參考文獻^[11]以掩護影像大小為 512 像素×512 像素、機密影像大小為 256 像素×256 像素之圖像，採用一階小波轉換及 VQ 壓縮技術可抵抗 JPEG 壓縮率至 40%，其 PSNR 值約為 15.03dB，但重建機密影像之清晰度已趨於模糊。

因此本文依參考文獻^[11]圖像大小之方式以三階小波轉換（掩護影像 Lena，機密影像 Airplane）及將機密影像設定壓縮條件為 Block Size 4×4，Codebook Size 256，其隱藏資料量為掩護影像大小

之 1/8 進行測試，當 JPEG 壓縮率於 40% 時，仍可完整取出機密影像；另本結果經 JPEG 壓縮 50% 時亦可完整取出機密影像且無雜點產生，而且我們得知經三階小波轉換後之機密影像對於抵抗 JPEG 壓縮可達 82%（如圖 10）時，仍可概略辨識出機密影像。

5. 結論

影像隱藏技術除了考慮機密影像及偽裝影像品質外，另需考慮其影像還原問題，當偽裝影像傳送接收端時可能遭受到破壞，而導致偽裝影像品質低落且隱藏於其中的索引值亦隨破壞程度而有所改變，所以使用已被破壞的索引值來還原機密影像，就會產生影像失真。因此在本文所採用的方法可以抵抗 JPEG 壓縮、裁切及馬賽克等破壞性試驗後，仍可將機密影像還原。

一般的影像在嵌入 3 個位元的機密影像時，人類視覺系統很難辨識出影像中的細微的變化。但是，當影像嵌入 4 個位元的機密影像時，灰階影像中比較平滑、內容變化程度比較小的區域裡，會有假輪廓（False Contouring）的現象發生。而且對於原有的灰階影像品質，將產生相當大的影響。因此在本文中以相同大小之影像做為實驗之依據，且考慮偽裝影像的不可發覺性、抗破壞能力及機密影像的重建品質，僅將 1/2 之掩護影像的資料量隱藏於最後 3 個位元之中，在二階轉換中我們將索引值隱藏至小波係數之最後第 1 及第 2 位元中；於三階轉換中我們將索引值隱藏至小波係數之最後第 2 及第 3 位元中，因此得到偽裝影像之 PSNR 值分別約為 37 dB 及 30 dB 左右。依據破壞試驗之結果，我們得到較佳的隱藏方式與強韌性，並證明本文採用三階小波轉換技術，於 15% 的 JPEG 壓縮率下能完整取回機密影像且無雜點產生並且能夠抵抗至少 50% 的 JPEG 壓縮、馬賽克、裁切等攻擊方式。

另將 512×512 像素之掩護影像做三階小波轉換，且隱藏 1/8 之掩護影像的資料量於小波係數之最後第 2 及第 3 位元中，得到此方式有較佳的抗破壞性，經 JPEG 壓縮 50% 可完整取出機密影像，且對於抗 JPEG 壓縮可達 82%，仍可概略辨識出機密影像。

參考文獻

- [1] Amdy, "Complementary Digital Watermarking Technique Based on Wavelet Transformation", Master's Thesis, Department of Electrical Engineering, National Chung-Hsing University, December 2001.
- [2] C. C. Chang and P. Y. Lin, "A compression-Based Data Hiding Scheme Using Vector Quantization and Principle Component Analysis", 2004 International Conference on Cyberworlds, pp. 369-375, November 2004.
- [3] C. S. Lu and H. Y. Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", IEEE Trans. Image Processing, Vol. 10, pp.1579-1592, October 2001.

- [4] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images", IEEE Trans. Image Processing, Vol. 8, pp58-68, January 1999.
- [5] H. C. Hsu, "Wavelet Base secure spread Spectrum Image Watermarking", Master's Thesis, Department of Electrical Engineering, National Chung-Hsing University, July 2003.
- [6] H. M. Lin, "The Design of Non-training Vector Quantization Codebook", Master's Thesis, Department of Information Management, National Central University, June 2002.
- [7] K. Sayhood, "Introduction to Data Compression", Morgan Kaufmann Publishers, pp. 183-185, pp.257-307, pp.455-495, 1996.
- [8] N. I. Wu, "A Study on Data Hiding for Gray-Level and Binary Images", Master's Thesis, Graduate Institute of Networking and Communication Engineering, Chao Yang University of Technology, May 2004.
- [9] S. C. Wu, "A Robust Halftone Binary Image Hiding Method", Master's Thesis, Department of Information Management, Chao Yang University of Technology, June 2003.
- [10] S. N. Chao, "Lossy-to-Lossless ECG Compression Using Wavelet Transform and a Unified Vector Quantization Framework", Master's Thesis, Department of Electronic Engineering, Chung Yuan Christian University Chungli, June 2004.
- [11] S. W. Guo, "Image Hiding Based on Hybrid VQ Compression and Discrete Wavelet Transformation", Master's Thesis, Department of Computer Science, National Chung-Hsing University, July 2004.
- [12] Y. C. Hu, "Gray-level image hiding scheme based on vector quantization", IEEE, Electronics Letters, Vol. 39, No. 2, pp. 202-203, January 2003.
- [13] Y. J. Lin, "A DWT-based and Effective Restoration Scheme for Tampered-with Image", Master's Thesis, Department of Information Management, Chao Yang University of Technology, July 2004.
- [14] Y. L. Luo, "Image Hiding with Message Authentication Code", Master's Thesis, Graduate Institute of Information Engineering, Feng Chia University, June 2004.
- [15] 陳同孝、張真誠、黃國峰,「數為影像處理技術」, 松岡電腦圖書資料股份有限公司, pp.8-1—8-18, 2001年1月。