

結合 IntDCT 與實對稱矩陣的多目標浮水印 A Multipurpose Watermarking Technique Using IntDCT and Real Symmetric Matrix

林正雄

萬能科技大學

資訊管理學系教授

jslin@vnu.edu.tw

林璟岑

萬能科技大學

資訊管理學系研究生

angel_linjt@hotmail.com

陳力銘

萬能科技大學

資訊管理學系研究生

ms0071799@hotmail.com

潘炳旺

陸軍專科學校

pan276551@gmail.com

摘要

本文採用 H.264 中的整數離散餘弦轉換 (Integer Discrete Cosine Transformation, IntDCT), 利用相鄰區塊係數之間特性, 藉由賀米特矩陣 (Hermitian Matrix) 的特徵值 (Eigenvalue) 與其所對應之特徵向量 (Eigenvectors), 產生一串數位簽章 (Signature Bits), 而數位簽章與浮水印分別嵌入 AC 與 DC 係數中, 以此加浮水印強健性與數位簽章的脆弱性。實驗證明, 本文所提出方法除了擁有好的影像品質, 在經過 JPEG 壓縮、切割、放大與縮小破壞後, 萃取出的浮水印具有很好辨識度, 同時也能夠精確定位被惡意竄改位置。

關鍵詞：多目標浮水印、整數離散餘弦轉換、賀米特矩陣

ABSTRACT

In this paper, we use Integer Discrete Cosine Transformation (IntDCT) which is used in the H.264 translate algorithm. The Eigenvalue and Eigenvector of Hermitian Matrix are generated for two coefficients corresponding to the same frequency in two different IntDCT blocks. At the signatures generation site, Signature bits are generated for the Eigenvalue and Eigenvector. In order to against the malicious attack such as noising, down scaling, and jpeg compressed, the watermarking is embedded into the DC coefficient. And signature bits are embedded into the AC coefficient in order to detect malicious manipulation on an image. Experimental results show that the performance of our multipurpose

watermarking scheme is indeed superb in terms of robustness and fragility.

Keywords: Watermarking, IntDCT, Hermitian Matrix

1 前言

欲保護資料完整性, 所使用技術為脆弱型浮水印 (Fragile Watermarking) [1-4], 許多學者已經對於此進行研究與應用, 但大多脆弱型浮水印都太過於靈敏與脆弱, 無法抵抗微小影像改變, 也無法容忍任何合法的影像處理, 例如 JPEG 壓縮。而 Lin 和 Chang[5]發現將影像 JPEG 壓縮後, 因為 JPEG 壓縮在高頻帶是以較大的係數量化, 而低頻帶是以較小的係數量化, 所以相鄰區塊的某些係數關係不變, 進而利用此特性求得其 signature bit 達到嵌入浮水印之目的。此系統因以 8x8 區塊為單位做嵌入, 偵測出來較不精確, 且浮水印對抗 JPEG 壓縮效果仍有進步的空間。

強健型浮水印 (Robust Watermarking) [6-9] 不論影像遭到壓縮、破壞或其它影像處理, 依然可以偵測出浮水印。多目的型浮水印 (Multipurpose Watermarking) [10-12]除了擁有脆弱型浮水印的優點, 也結合強健型浮水印特性, 在萃取浮水印後仍具有識別版權能力, 也能精確偵測數位媒體使破壞位置。現今, 多目的型浮水印系統面臨挑戰, 要能兼顧到影像品質, 且能在各種影像處理攻擊下, 仍完整的保留住浮水印資訊, 同時偵測出影像遭受到惡意破壞的部分。

本文利用賀米特矩陣 (Hermitian Matrix) 的特徵值與對應特徵向量產生一串簽章位元

(Signature Bits)，將簽章位元(Signature Bits)嵌入 AC 中，並以此偵測浮水印是否被惡意攻擊，而浮水印嵌入 DC 中以增加其強健性，做為保護智慧財產權的依據。實驗證明本文所提出的多目的型浮水印系統，除了擁有好的影像品質，在經過 JPEG 壓縮、切割、放大與縮小等破壞，萃取出的浮水印仍具有很好的辨識度，同時也能夠精確定位被惡意竄改位置。

本文分為五章；第一章為緒論，說明實驗背景、動機與方向。第二章在說明整數離散餘弦轉換與賀米特矩陣。第三章將先介紹本文提出之浮水印技術。第四章是系統實驗結果。第五章為結論與未來方向。

2 整數離散餘弦轉換與賀米特矩陣

2.1 整數離散餘弦轉換(Integer Discrete Cosine Transformation, IntDCT)

ISO 與 ITU 從 1990 年代開始制定一序列的影音訊號編碼標準，ITU 制定 H.261/262/263/264 標準，ISO 則制定 MPEG-1/2/4 標準，兩者之間互有交錯重疊。目前最新一代的 H.264 視訊編碼壓縮規格為 ITU-T (VCEG) 與 ISO / IEC (MPEG) 共同組成的 (JVT) 所制訂的視訊壓縮標準。在轉換編碼方面，使用 4×4 區塊的整數離散餘弦轉換(Integer Discrete Cosine Transformation, IntDCT)，有別於原有視訊編碼規格 8×8 區塊的離散餘弦轉換(Discrete Cosine Transformation, DCT)。在轉換的乘法運算中，僅需要加法和位元平移運算，因此減低了計算複雜度與截尾誤差所造成的區塊效應[13-16]。

IntDCT 轉換公式如公式(1)(2)，公式(1)為空間域轉頻率域；而公式(2)為頻率域轉乘空間域。其中：Y 指頻率域之係數位置、X 指空間域的像素位置。

整數離散餘弦轉換(IntDCT)與離散餘弦轉換(DCT)有著相同的物理特性，其中頻率與能量分佈的情況也是相同，兩者間的差別為區塊大小，從 8×8 轉變為 4×4。

2.2 賀米特矩陣(Hermitian Matrix)

對稱矩陣(Symmetric Matrix) $M^T=M$ 是所有實數矩陣中應用最廣泛的特殊矩陣。對稱矩陣有實數特徵值(Eigenvalue)，也有完整的一組正交且正規特徵向量，因此對稱矩陣可被正交對角化， $M=QAQ^T$ ，其中 A 為主對角特徵值矩陣，Q 為正交特徵向量矩陣(即 $Q^{-1}=Q^T$)。

複數矩陣也存在與實數對稱矩陣相應的矩陣，稱為賀米特矩陣(Hermitian Matrix)，它是落在複數的向量空間中，而且是一個對稱且正交的矩陣。

若矩陣 M 中之元素 $\bar{a}_{ij}=a_{ji}$ ，稱為賀米特矩陣，通常記為 M^* 或 M^H ，如公式(3)所示。

簡單來說，令 $M=A+IB$ ，將矩陣 M 進行共軛運算，運算後定義為 $\bar{M}=A-IB$ ，接著將 $\bar{M}$ 進行轉置運算，運算後定義成 M^H 或 M^* ，只要符合 $M=M^H$ 或 $M=M^*$ ，即為賀米特矩陣。它有四個重要性質如下：

- 令 M 是賀米特矩陣，對於任意向量 X， X^*MX 是實數。
- 賀米特矩陣的特徵值(Eigenvalue)皆為實數。
- 賀米特矩陣所對應相異特徵值(Eigenvalue)的特徵向量(Eigenvectors)互為正交。
- 可單位對角化(Unitarily diagonalizable)。

$$Y = (C_f \times X \times C_f^T) \otimes E_f \quad (1)$$

C_f 、 E_f 、a、b 分別如下：

$$C_f = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{bmatrix}, \quad E_f = \begin{bmatrix} a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \\ 2 & \frac{4}{ab} & 2 & \frac{4}{ab} \\ a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \end{bmatrix}$$

$$a = \frac{1}{2}, b = \sqrt{\frac{5}{2}}$$

$$X = C_i^T \times (Y \otimes E_i) \times C_i \quad (2)$$

C_i 、 E_i 、a、b 分別如下：

$$C_i = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \frac{1}{2} & -\frac{1}{2} & -1 \\ 1 & -1 & -1 & 1 \\ \frac{1}{2} & -1 & 1 & -\frac{1}{2} \end{bmatrix}, \quad E_i = \begin{bmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \end{bmatrix}$$

$$a = \frac{1}{2}, b = \sqrt{\frac{5}{2}}$$

$$M=[a_{ij}]_{2 \times 2} = \begin{bmatrix} 4 & 2-3i \\ 2+3i & 5 \end{bmatrix} \quad (3)$$

3 嵌入、偵測與驗證

本文嵌入程序採用[17]學者所提出之方法加以改良，首先將原始影像經整數離散餘弦轉換 (IntDCT) 將影像轉為頻域率，利用賀米特矩陣 (Hermitian Matrix) 的特徵值與特徵向量以產生數位簽章 (Digital Signature)，將數位簽章 (Digital Signature) 嵌入於影像 AC 係數中，將強健型浮水印以亂數種子打亂，嵌入於影像 DC 係數中。

3.1 產生數位簽章

步驟一：將賀米特矩陣 (Hermitian Matrix) H 定義如下。

$$H=M^T \times M$$

$$M=[a_{xy}]; x,y=1,2$$

步驟二：將影像分割成大小為 4x4 不重疊之區塊，每區塊進行整數離散餘弦轉換 (IntDCT)，使影像從空間域轉換為頻域率。

步驟三：本文中 l 與 m 分別選擇 1、2，偏離值 B 選擇 3[6]。在相鄰區塊 p、q 中，兩區塊中的 AC(1,1)、AC(1,2)、AC(2,1) 與 AC(2,2) 設為 $f_p(i,j)$ 與 $f_q(i,j)$, $i,j=1,2$ ，以公式 (4) 產生出 M，將 $M^T \times M$ 得到賀米特矩陣 (Hermitian Matrix) H。

步驟四：計算出賀米特矩陣 (Hermitian Matrix) H 之特徵向量 $[x,y]^T$ ，在由公式(5)得到相對應之角度 θ 。

步驟五：由角度 θ 參照表 3-1，找出此區塊之 Signature bits。

$$a_{xy} = \begin{cases} 1 & \text{if } f_p(i,j) - f_q(i,j) + B \geq 0 \\ m & \text{if } f_p(i,j) - f_q(i,j) + B < 0 \end{cases} \quad i,j=1,2 \quad (4)$$

其中 f_p 與 f_q 為相鄰區塊 p 與 q 中之低頻係數，B 為偏離值

$$\theta = \tan^{-1} \frac{y}{x}, \quad 0^\circ \leq \theta \leq 90^\circ \quad (5)$$

其中 f_p 與 f_q 為相鄰區塊 p 與 q 中之低頻係數，B 為偏離值

表 3-1 Signature bits and direction of dominant eigenvector.

Signature bits	001	010	011	100
θ	26.56°	31.71°	37.98°	45°
Signature bits	101	110	111	
θ	52.01°	58.28°	63.43°	

3.2 嵌入數位簽章

步驟一：在影像的頻域率中，IntDCT_{AC_Value}

為 IntDCT 係數交流部分，當我們判斷相鄰兩區塊 f_p 、 f_q 的關係後，將 IntDCT_{AC_Value} 係數中 AC(1,2)、AC(2,1) 與 AC(2,2) 分別除以固定量化值 Q 如公式 (6) (7)，其中量化後根據兩區塊之特性做無條件捨去 (Floor) 或無條件進位 (Ceil)，此做法為了維持兩區塊之係數關係，最後量化得到係數 κ_p 與 κ_q 。

步驟二：將 Signature bits 複製兩份 γ_p 與 γ_q ，嵌入相鄰兩區塊 IntDCT_{AC_Value} 係數中的 AC(1,2)、AC(2,1)、AC(2,2) 與 IntDCT'_{AC_Value} 係數中的 AC(1,2)、AC(2,1)、AC(2,2)，分別以公式(8)、(9)嵌入。

$$\kappa_p = \begin{cases} \left\lceil \frac{\text{IntDCT}_{AC_Vale}}{Q} \right\rceil & \text{if } f_p - f_q + B \geq 0 \\ \left\lfloor \frac{\text{IntDCT}_{AC_Vale}}{Q} \right\rfloor & \text{if } f_p - f_q + B < 0 \end{cases} \quad (6)$$

$$\kappa_q = \begin{cases} \left\lceil \frac{\text{IntDCT}'_{AC_Vale}}{Q} \right\rceil & \text{if } f_p - f_q + B \geq 0 \\ \left\lfloor \frac{\text{IntDCT}'_{AC_Vale}}{Q} \right\rfloor & \text{if } f_p - f_q + B < 0 \end{cases} \quad (7)$$

$$\text{IntDCT}_{AC_Vale} = \begin{cases} \kappa_p * Q \text{ if } (\gamma_p = 0) \text{ and } (\kappa_p \text{ is even}) \\ \kappa_p * Q + Q \text{ if } (\gamma_p = 0) \text{ and } (\kappa_p \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ \kappa_p * Q - Q \text{ if } (\gamma_p = 0) \text{ and } (\kappa_p \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \\ \kappa_p * Q \text{ if } (\gamma_p = 1) \text{ and } (\kappa_p \text{ is odd}) \\ \kappa_p * Q + Q \text{ if } (\gamma_p = 1) \text{ and } (\kappa_p \text{ is even}) \text{ and } (f_p - f_q + B \geq 0) \\ \kappa_p * Q - Q \text{ if } (\gamma_p = 1) \text{ and } (\kappa_p \text{ is even}) \text{ and } (f_p - f_q + B < 0) \end{cases} \quad (8)$$

$$\text{IntDCT}_{AC_Value}' = \begin{cases} \kappa_q * Q \text{ if } (\gamma_q = 0) \text{ and } (\kappa_q \text{ is even}) \\ \kappa_q * Q - Q \text{ if } (\gamma_q = 0) \text{ and } (\kappa_q \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ \kappa_q * Q + Q \text{ if } (\gamma_q = 0) \text{ and } (\kappa_q \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \\ \kappa_q * Q \text{ if } (\gamma_q = 1) \text{ and } (\kappa_q \text{ is even}) \\ \kappa_q * Q - Q \text{ if } (\gamma_q = 1) \text{ and } (\kappa_q \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ \kappa_q * Q + Q \text{ if } (\gamma_q = 1) \text{ and } (\kappa_q \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \end{cases} \quad (9)$$

3.3 嵌入浮水印

步驟一：在影像的頻域率中，相鄰兩區塊

IntDCT_{AC_Value} 中的 $AC(1,1)$ 、 $AC(1,2)$ 、 $AC(2,1)$ 與 $\text{IntDCT}_{AC_Value}'$ 中的 $AC(1,1)$ 、 $AC(1,2)$ 、 $AC(2,1)$ ，設為 f_p 與 f_q 。

步驟二：嵌入浮水印前，將二維的浮水印影像 W 轉換成一維的浮水印序列 $S(k)$ ， $k=0,1,2,\dots,(m*n)-1$ ，其中 $m*n$ 為浮水印大小。使用重複編碼的方式，把原始信號加以重複 N 次，假設原始信號為 S ，則編碼後的訊號 $\omega = \{s, s, \dots, s\}$ ，共 n 個 S ，最後將浮水印 ω 以亂數種子打散，以抵抗區域破壞。

步驟三：令 IntDCT_{DC_Value} 為 IntDCT_{AC_Value} 中的 $AC(1,1)$ ，是 IntDCT 係數直流部分，判斷相鄰兩區塊 f_p 、 f_q 的關係後，將 IntDCT_{DC_Value} 係數除以固定量化值 Δ 如公式(10)(11)，在以無條件捨去(Floor)或無條件進位(Ceil)，此做法為了維持兩區塊之係數關係，最後求出量化後係數 T_p 與 T_q 。

步驟四：令對應兩區塊之浮水印為 ω_p 與 ω_q ，分別嵌入相鄰兩區塊 IntDCT_{DC_Value} 係數與 $\text{IntDCT}_{DC_Value}'$ ，以公式(12)、(13)嵌入。

步驟五：將嵌入數位簽章與浮水印之影像以逆整數離散餘弦轉換 (IntDCT) 進行運算，使影像轉回成空間域。

$$T_p = \begin{cases} \left\lceil \frac{\text{IntDCT}_{DC_Value}}{\Delta} \right\rceil & \text{if } f_p - f_q + B \geq 0 \\ \left\lfloor \frac{\text{IntDCT}_{DC_Value}}{\Delta} \right\rfloor & \text{if } f_p - f_q + B < 0 \end{cases} \quad (10)$$

$$T_q = \begin{cases} \left\lceil \frac{\text{IntDCT}_{DC_Value}}{\Delta} \right\rceil & \text{if } f_p - f_q + B \geq 0 \\ \left\lfloor \frac{\text{IntDCT}_{DC_Value}}{\Delta} \right\rfloor & \text{if } f_p - f_q + B < 0 \end{cases} \quad (11)$$

$$\text{IntDCT}_{DC_Value}' = \begin{cases} T_p * \Delta \text{ if } (\omega_p = 0) \text{ and } (T_p \text{ is even}) \\ T_p * \Delta + \Delta \text{ if } (\omega_p = 0) \text{ and } (T_p \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ T_p * \Delta - \Delta \text{ if } (\omega_p = 0) \text{ and } (T_p \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \\ T_p * \Delta \text{ if } (\omega_p = 1) \text{ and } (T_p \text{ is even}) \\ T_p * \Delta + \Delta \text{ if } (\omega_p = 1) \text{ and } (T_p \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ T_p * \Delta - \Delta \text{ if } (\omega_p = 1) \text{ and } (T_p \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \end{cases} \quad (12)$$

$$\text{IntDCT}_{DC_Value}' = \begin{cases} T_q * \Delta \text{ if } (\omega_q = 0) \text{ and } (T_q \text{ is even}) \\ T_q * \Delta - \Delta \text{ if } (\omega_q = 0) \text{ and } (T_q \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ T_q * \Delta + \Delta \text{ if } (\omega_q = 0) \text{ and } (T_q \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \\ T_q * \Delta \text{ if } (\omega_q = 1) \text{ and } (T_q \text{ is even}) \\ T_q * \Delta - \Delta \text{ if } (\omega_q = 1) \text{ and } (T_q \text{ is odd}) \text{ and } (f_p - f_q + B \geq 0) \\ T_q * \Delta + \Delta \text{ if } (\omega_q = 1) \text{ and } (T_q \text{ is odd}) \text{ and } (f_p - f_q + B < 0) \end{cases} \quad (13)$$

3.4 驗證程序

步驟一：與嵌入程序中產生數位簽章方法相同，將影像分割成大小為 4×4 不重疊區塊，每區塊進行整數離散餘弦轉換 (IntDCT)，使待驗證影像轉換為頻域率，在從相鄰兩區塊 $AC(1,1)$ 、 $AC(2,1)$ 、 $AC(1,2)$ 、 $AC(2,2)$ 中產生三位元之 Signature Bits，令為 γ'_{new} 。

步驟二：從相鄰區塊 IntDCT_{AC_Value} 係數中的 $(1,2)$ 、 $AC(2,1)$ 、 $AC(2,2)$ 與 $\text{IntDCT}_{AC_Value}'$ 係數中的 $AC(1,2)$ 、 $AC(2,1)$ 、 $AC(2,2)$ ，以公式(14)取出已嵌入三位元之 Signature bits 兩份，設為 γ'_p 與 γ'_q (由於兩區塊嵌入同一份 Signature Bits，因此萃取出兩份的 Signature bits)。

步驟三：若 γ'_p 、 γ'_q 中有一組與待驗證影像區塊中產生的 Signature Bits 不同，表示未通過認證，此區塊視為被遭到惡意竄改，若相同則表示此區塊未遭到惡意攻擊，將驗證區塊結果記錄成 F ，如公式(15)所示。

3.5 萃取程序

步驟一：在待驗證影像的頻域率中，每區塊的 $\text{IntDCT}_{\text{DC_Value}}$ 以公式(16)，即可取出浮水印 ω' 。

步驟二：以亂數種子將打亂的 ω' 序列還原成 $\omega'(k)=\{S_1, S_2, \dots, S_N\}$ ，其中 S 為重複編碼還原後的浮水印， N 為重複編碼的次數。

3.6 浮水印錯誤修正(Error-Correcting)

步驟一：以公式 (17) 進行投票，將浮水印 ω' 投票取出得到 ω_{new} ，其中得到相同投票數浮水印設為-1。

步驟二：將投票完的一維浮水印序列轉換成二維浮水印影像。

步驟三：將浮水印中為-1(票數相同)的 ω_{new} ，以公式(18)進行均化運算。

$$\gamma' = \begin{cases} 0 & \text{if } \text{round}\left(\frac{\text{IntDCT}_{\text{ACvalue}}}{Q}\right) = \text{even} \\ 1 & \text{if } \text{round}\left(\frac{\text{IntDCT}_{\text{ACvalue}}}{Q}\right) = \text{odd} \end{cases} \quad (14)$$

$$F = \begin{cases} 1 & \text{if } \gamma'_p \neq \gamma'_{\text{new}} \quad \text{or} \quad \gamma'_q \neq \gamma'_{\text{new}} \\ 0 & \text{if } \gamma'_p = \gamma'_{\text{new}} \quad \text{and} \quad \gamma'_q = \gamma'_{\text{new}} \end{cases} \quad (15)$$

$$\omega' = \begin{cases} 1 & \text{if } \text{round}\left(\frac{\text{IntDCT}_{\text{DCvalue}}}{\Delta}\right) = \text{even} \\ 0 & \text{if } \text{round}\left(\frac{\text{IntDCT}_{\text{DCvalue}}}{\Delta}\right) = \text{odd} \end{cases} \quad (16)$$

$$\omega_{\text{new}} = \begin{cases} 1 & \text{if } S > n/2 \\ 0 & \text{if } S < n/2 \\ -1 & \text{if } S = n/2 \end{cases} \quad (17)$$

其中 $S = \sum_{k=1}^n \omega'(k)$ ， n 為浮水印重複次數

$$\omega_{\text{new}} = \begin{cases} 1 & \text{if } S \geq 0.5 \\ 0 & \text{if } S < 0.5 \end{cases} \quad (18)$$

其中 ρ 為 ω_{new} 周邊 3×3 區塊， $S = \frac{1}{8} \sum_{k=1}^8 \rho(k)$

Noise Ratio, PSNR) 來做為衡量工具[18]。若兩張影像經 PSNR 計算結果值越大，表示兩張影像越相似，也可以說失真越少。一般來說若 PSNR 大於 30 以上，表示用肉眼難以分辨兩張圖片。

公式 (19) 為整個影像之誤差平方總和，其中 $g(x,y)$ 為經過修改的影像， $h(x,y)$ 為原始影像。公式 (20) 為兩張 $M \times N$ 灰階影像的均方差 (Mean Square Error, MSE)，其中 $M \times N$ 為影像大小。公式 (21) 為影像信號雜訊比 (PSNR) 的公式。

4.2 正規化關聯值(Normalized Correlation, NC)

本論文以正規化關聯值 (Normalized Correlation, NC) 作為萃取後浮水印與原始浮水印的衡量標準。公式 (22) 為正規化關聯值 (NC) 的公式，其中 W 為原始浮水印， W' 為萃取後浮水印。當 NC 值為 1 時，表示兩浮水印相同，而 NC 值小於 0.7 時，表示用肉眼觀察已相當模糊。

$$e(x, y) = g(x, y) - h(x, y) \quad (19)$$

$$\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [g(x, y) - h(x, y)]^2 \quad (20)$$

$$PSNR(db) = 10 \log_{10} \frac{I_{\text{max}}^2}{\frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [g(x, y) - h(x, y)]^2} \quad (21)$$

$$NC = \frac{\sum_i \sum_j W(i, j) W'(i, j)}{\sum_i \sum_j [W(i, j)]^2} \quad (22)$$

，其中 $0 \leq NC \leq 1$

4.3 實驗結果

本文採用六張測試影像，影像大小為 512×512 ，分別為 Baboon、F16、Goldhill、Lena、Pepper 與 Scene。浮水印方面，由 64×64 二元影像做重複編碼四次作為本實驗之浮水印。

在 AC 係數嵌入數位簽章時只需做細微調

4 實驗結果

4.1 影像信號雜訊比 (Peak Signal to Noise Ratio, PSNR)

用人類肉眼很難判斷出影像好壞，因此大多學者是使用影像信號雜訊比 (Peak Signal to

整，因此本實驗將 AC (2,1)、AC (1,2)、AC (2,2) 量化值 Q 設定為 3，DC 係數部分嵌入浮水印，整大小決定浮水印強健性與影像品質，本文由圖 4-1 選擇三種影像品質代表， $\Delta=12$ 、 $\Delta=44$ 與 $\Delta=76$ 。

在影像品質方面，由表 4-1 可以發現，DC 量化值 $\Delta=12$ 、 $\Delta=44$ 、 $\Delta=76$ 均有很好的影像品質。在抗攻擊方面，由表 4-2 顯示 Δ 越大，能抵抗 JPEG 壓縮能力也越好，其中 $\Delta=44$ 可抵抗 JPEG 40% 以上的攻擊，而 $\Delta=76$ 更可達到 JPEG 20% 以上。切割攻擊會將影像的資訊流失，由表 4-3 可以看出 DC 量化值 Δ 的大小和萃取出浮水印之品質無關聯，在切割後剩餘資訊 50% 後仍可以有效的識別版權能力。由表 4-4 可以發現 Δ 越大，抵抗倍率縮放攻擊能力也越好，除縮小 0.2 倍攻擊所萃取出浮水印效果較不佳之外，其餘均有很好的影像品質。由表 4-5 可看出，雜訊的比例影響萃取出浮水印品質，DC 量化值 Δ 的大小和萃取出浮水印之品質無關聯，在 7% 以下的胡椒鹽雜訊攻擊，浮水印皆可判別版權。

在驗證方面，由圖 4-2、圖 4-3、圖 4-4、圖 4-5 可以明顯看出，本文使用 4x4 整數離散餘弦轉換 (IntDCT) 與利用特徵向量的正交特性，對於竄改的區域可以精確定位被竄改位置。

5 結論與未來工作

本文採用 H.264 之 4x4 區塊為單位的整數離散餘弦轉換 (IntDCT)，有別於其他學者使用 8x8 區塊為單位的離散餘弦轉換 (DCT)，最大差別就是能嵌入更大的資料量，同時擁有好的影像品質。實驗結果顯示，當受到惡意攻擊時，能正確檢測，同時也更精確定位被竄改位置。不論影像經過 JPEG 壓縮、切割、放大與縮小等破壞，萃取出浮水印具有很高的辨識度，可做為保護版權的依據，但由於本文浮水印是以量化 DC 係數方式嵌入，因此無法抵

抗對能量大幅度的改變與相對位置改變的攻擊，希望未來能努力朝此方向克服。

表 4-1 六張影像在 DC 量化值 $\Delta=12$ 、 $\Delta=44$ 、 $\Delta=76$ 之 PSNR

Picture \ PSNR	$\Delta=12$	$\Delta=44$	$\Delta=76$
Baboo	52.3925	41.0790	36.3837
F16	52.2935	41.1874	36.4212
Goldhill	52.3687	41.1939	36.4076
Lena	52.2817	41.0589	36.3261
Pepper	52.3354	41.2022	36.5430
Scene	52.3265	41.1126	36.3731
Average	52.3331	41.1390	36.4091

表 4-2 $\Delta=12$ 、 $\Delta=44$ 、 $\Delta=76$ 經 JPEG 攻擊，萃取出浮水印之 NC 值結果

JPEG	$\Delta=12$	$\Delta=44$	$\Delta=76$
QF: 100%	1.0000	1.0000	1.0000
QF: 90%	0.9625	1.0000	1.0000
QF: 80%	0.5618	1.0000	1.0000
QF: 70%	0.3673	0.9981	1.0000
QF: 60%	0.3205	0.9889	1.0000
QF: 50%	0.3219	0.9226	0.9986
QF: 40%	0.3548	0.8268	0.9935
QF: 30%	0.3617	0.5461	0.9528
QF: 20%	0.5016	0.3136	0.7128
QF: 10%	0.4335	0.4201	0.2853

表 4-3 $\Delta=12$ 、 $\Delta=44$ 、 $\Delta=76$ 經切割攻擊，萃取出浮水印之 NC 值結果

切割剩餘比例	$\Delta=12$	$\Delta=44$	$\Delta=76$
90%	1.0000	1.0000	1.0000
80%	0.8884	0.9195	0.8902
70%	0.8597	0.9991	0.8569
60%	0.8221	0.8713	0.8189
50%	0.7406	0.8578	0.7411

表 4-4 $\Delta=12$ 、 $\Delta=44$ 、 $\Delta=76$ 經倍率縮放攻擊，萃取出浮水印之 NC 值結果

倍率縮放	$\Delta=12$	$\Delta=44$	$\Delta=76$
0.25	0.3312	0.2784	0.2728
0.5	0.5651	0.9551	0.9903
0.75	0.9880	1.0000	1.0000
1.25	0.9991	1.0000	1.0000
1.75	0.9935	1.0000	1.0000

2	0.9972	1.0000	1.0000
5	0.9977	1.0000	1.0000
10	0.9977	1.0000	1.0000

表 4-5 $\Delta=12$ 、 $\Delta=44$ 、 $\Delta=76$ 經胡椒鹽雜訊攻擊，萃取浮水印之 NC 值結果

胡椒鹽雜訊	$\Delta=12$	$\Delta=44$	$\Delta=76$
1%	0.9949	0.9954	0.9958
3%	0.9254	0.9254	0.9398
5%	0.8268	0.7809	0.8069
7%	0.6702	0.6063	0.6665

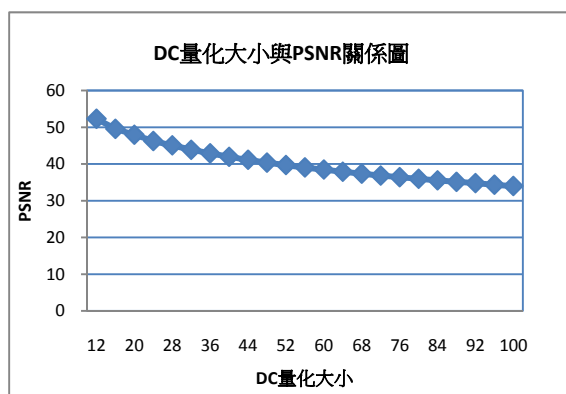


圖 4-1 六張影像在 DC 量化值 Δ 各種情況下 PSNR 平均值

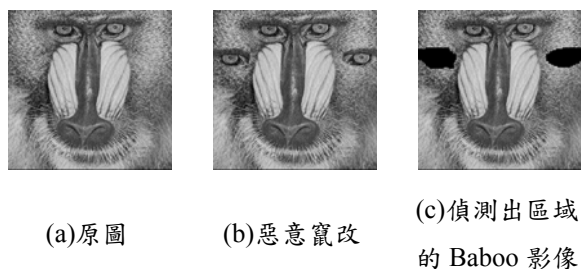


圖 4-2 惡意竄改的 Baboo 影像

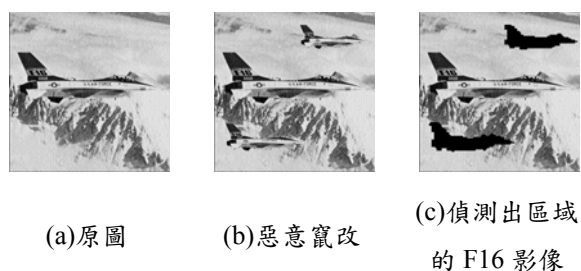
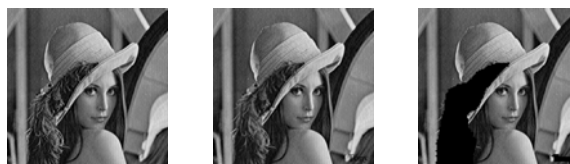
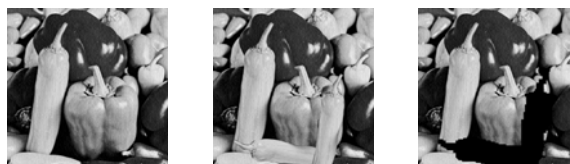


圖 4-3 惡意竄改的 F16 影像



(a)原圖 (b)惡意竄改 (c)偵測出區域的 Lena 影像

圖 4-4 惡意竄改的 Lena 影像



(a)原圖 (b)惡意竄改 (c)偵測出區域的 Pepper 影像

圖 4-5 惡意竄改的 Pepper 影像

6 參考文獻

- [1] Cong Jin, Yan Chao, Xiao-Liang Zhang, "Semi-Fragile Watermark Based on Adaptive Quantization for Image Content Authentication", International Conference on E-Business and Information System Security, pp.1-5, 2009.
- [2] Liangbin Zheng and Fucheng You, "A Fragile Digital Watermark Used to Verify the Integrity of Vector Map", International Conference on E-Business and Information System Security, pp.1-4, 2009.
- [3] A.H. Sulaiman and F.S. Baji, "Fractal Based Fragile Watermark", Second International Conference on Computer and Electrical Engineering, vol.2, pp.139-143, 2009.
- [4] Liangbin Zheng, Yeli Li, Liuping Feng and Huaqun Liu, "Research and implementation of fragile watermark for vector graphics", 2010 2nd International Conference on Computer Engineering and Technology (ICCET), vol.1, pp.522-525, 2010.
- [5] C.-Y. Lin and S.-F. Chang, "Semi-fragile

- watermarking for authenticating JPEG visual content”, Proc. SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, pp. 140-151, January 2000.
- [6] A. Mairgiotis, N.Galatsanos and Yongyi Yang,” Robust watermark detection based on a new spatially weighted total variation based image prior”, International Conference on Symposium ELMAR, pp.45-48, 2009.
- [7] Cong Jin, Shi-Hui Wang, Shu-Wei Jin, Qing-Guo Zhang and Jun-Min Ye, “Robust Digital Watermark Technique for Copyright Protection”, International Symposium on Information Engineering and Electronic Commerce, pp.237-240, 2009.
- [8] Gao Hai-ying, Liu Guo-qiang, Li Xu, Xu Yin, “A Robust Watermark Algorithm for JPEG2000 Images”, 2009. IAS '09. Fifth International Conference on Information Assurance and Security, vol.2, pp. 230-233, 2009.
- [9] Hai-Yan Yu, Jiu-Lun Fan and Xiao-Li Zhang, ” A Robust Watermark Algorithm Based on Ridgelet Transform and Fuzzy C-Means”, International Symposium on Information Engineering and Electronic Commerce, pp.120-124, 2009.
- [10] Congxu Zhu and Yuping Hu, “A Multipurpose Watermarking Scheme for Image Authentication and Copyright Protection”, 2008 International Symposium on Electronic Commerce and Security, pp. 930-933, 2008.
- [11] Yu-Wen Ding, Zi Lin, Li Wang, “A Multipurpose Public-Key Cryptosystem Based Image Watermarking”, 4th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2008.
- [12] Min-Jen Tsai, Chang-Hsing Shen, Jung Liu, “Multipurpose Image Watermarking Based on the Wavelet Tree Contrast Level Transformation”, IEEE International Conference on Communications, pp. 1-4, 2009.
- [13] ISO/IEC International Standard 11172-2, Information technology – Coding of moving pictures and associated audio for digital storage media up to about 1.5 Mbits/s – Part 2: Video, first edition, Aug. 1993.
- [14] ISO/IEC International Standard 13818-2, Generic coding of moving pictures and associated audio – Part 2: Video, 1995.
- [15] ITU-T Recommendation H.261, Video Codec for Audiovisual Services at p x 64 kbit/s, March 1993.
- [16] J. Zhagn, Anthony T. S. Ho, ”An efficient digital image-in-image watermarking algorithm using the integer discrete cosine transform (IntDCT),” ICICS-PCM 2003, vol. 2, Singapore, 15-18 Dec. 2003, pp. 1163-1167.
- [17] Ching-Tang Hsieh, Yeh-Kuang Wu, Kuo-Ming Hung, “Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix”, Tamkang Journal of Science and Engineering, vol 10, No.3, September 2007, pp.211-220.(EI)
- [18] Y. Choi, I. Aizawa, ”Digital watermarking using inter-block correlation,” in Proc. International Conf. on Image Processing, vol. 2, October 1999, pp.216-220.