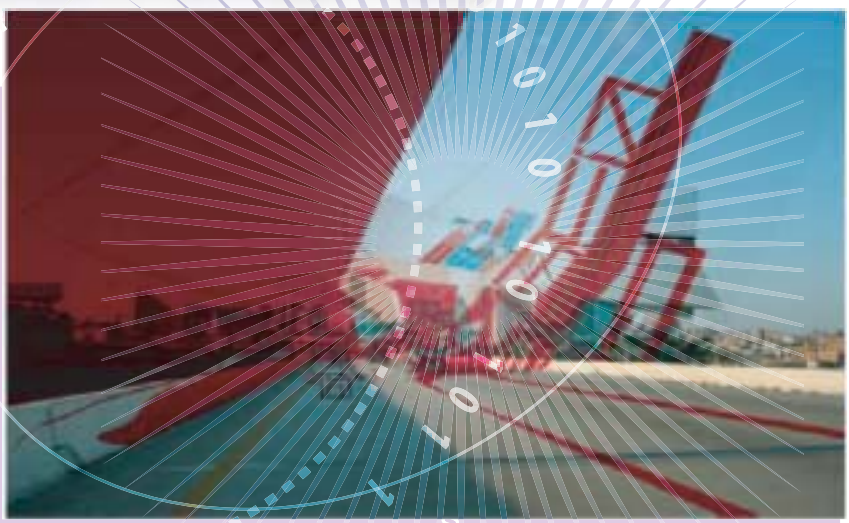
適用於JPEG2000影像壓縮標準資訊隱藏技術之探討

作者/周兆龍 上尉
婁德權 上校



提要

2001年美國紐約世貿大樓遭到以奧薩瑪．賓拉登為首的恐怖份子攻擊，美國國家安全部門經過深入調查後發現，賓拉登等人極可能透過網站或視訊作為指示不法活動的途徑。這類利用多媒體資料隱藏秘密資訊的方法，與傳統加密技術不同，不僅讓人無法感受其是否存在，在現今資訊爆炸的時代，更難有效的蒐集可能隱藏秘密資訊的資料。這次的恐怖攻擊，除了造成世人的震撼，更引起世界各國對於資訊隱藏技術的重視。

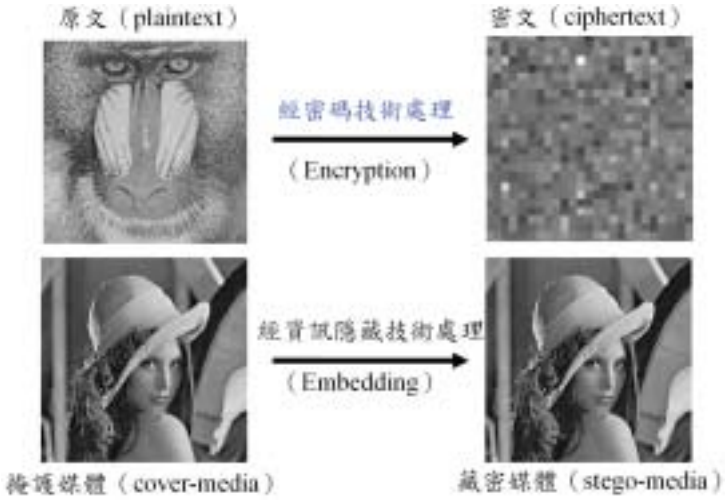
資訊隱藏技術是指將不欲人知的秘密資訊藏入一般看似正常的資料，可應用於軍事、商業、政府或個人隱私等各種範疇。本文將以目前網際網路上最常使用的數位影像做為探討的範圍，說明資訊隱藏技術在數位影像上的應用原理，並針對新一代數位影像壓縮標準JPEG2000的壓縮編碼特性，研究如何設計研發以符合其應用的資訊隱藏技術。

前言

從前人們曾利用各種方式來傳送秘密資訊①，例如中國古代有將秘密訊息寫在絲帶上，捲成球狀後裹上一層蠟，再交由信差吞下後傳送；古希臘人將信差的頭髮剃光後，刺上秘密訊息，等信差頭髮長出後，再令其傳送信息；二次世界大戰中，德國人所發明的微點(microdots)技術，有效的將秘密情報縮小在英文字母小寫"i"的小點中，而透過一般文件大量的傳送；另外隱形墨水(Invisible Inks)由於取材製作容易，只需將一般信紙加熱即可顯現秘密訊息，在二次世界大戰初期也被廣泛的使用。

從這些資訊隱藏的例子，可以瞭解資訊隱藏技術實際上是利用了各種方式，將欲傳送的秘密資訊隱藏在人們所不易察覺的位置。資訊隱藏與加密技術的不同之處，就是加密後的資料通常已成爲沒有意義的亂碼；而經過藏密後的資料，由於不去改變原本的資料型態，因此在傳輸過程中，使人無法感

① S. Katzenbeisser, F. A. P. Petitcolas, "Information hiding techniques for steganography and digital watermarking," Artech House, Boston, 2000.



圖一　密碼技術與資訊隱藏技術比較圖 (作者繪製)

覺出秘密資訊的存在(如圖一所示)。

通常我們將用以藏入秘密資訊的媒體稱爲掩護媒體(cover-media)，資訊隱藏的動作稱爲嵌入(embedding)，經嵌入秘密資訊後的資料則稱爲載密媒體(stego-media)。

一般資訊隱藏技術具有以下幾種特性：

一、不可察覺性(imperceptibility)

隱藏之資訊要讓人難以發覺，通常與人眼視覺特性相關。

二、強固性(robustness)

藏入之資訊要對於合法使用者的一般處理(如壓縮、雜訊干擾與檔案格式轉換等)或非法者的惡意破壞，均可取出隱藏的資訊。

三、容量(capacity)

在不可察覺性的前提下，能藏入愈多的秘密資訊愈好。

四、安全性(security)

隱藏之資訊不可輕易被偵測出，即使已偵測得知內含隱藏資訊，也不能輕易移除。

這些特性彼此間存在著取捨(trade-off)的關係，例如要求不可察覺性高，則相對所藏入的資料容量要減少；而若爲了提高藏入的資料，則可能降低其強固性。

現今泛指的資訊隱藏技術，依據應用範疇的不同，可以概略分成以下四類②：

一、秘密通道(Covert Channel)

意指在電腦系統中，存在著系統管理者無法察覺的通道，單位內部的非法人員可能透過這種通道將系統中的秘密資訊洩漏出去。例如監看程式或Cookie。

二、匿名(anonymity)

意指在傳輸訊息時，傳送方或接收方隱藏其相關訊息，讓人無法有效追蹤來源。例如匿名瀏覽網站訊息或發送匿名電子郵件。

三、藏密學(steganography)

意指在不破壞掩護媒體的情況下，將秘密資訊藏入其中，而使得藏密媒體在傳輸或使用的過程中，讓人無法察覺其中已隱藏秘密資訊。

四、著作權標示(Copyright Marking)

意指在具有版權的智慧財產資料中，加入代表合法版權的資訊，可以用來宣告版權或者追蹤非法使用者。例如數位浮水印(Digital Watermarking)。

其中藏密學與數位浮水印技術是最常被研究討論的領域。通常藏密學被使用在點對點(point-to-point)的通訊中，其基本要求就是希望能藏入大量的秘密資訊而不被發覺，不可察覺性與容量是最重要的要求。數位浮

② F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol. 87, no. 7, July 1999, pp.1062-1078.

水印通常使用在一對多的通訊，其基本要求是希望藏入的資料不會在正常使用情況下，或甚至遭惡意移除而被破壞，因此強固性是最重要的要求。

藏密學可以應用在各種軍事、情報、電子商務或政府公務，並且可與通訊的展頻(Spread Spectrum)技術搭配，應用在各種秘密通訊。數位浮水印技術則常應用在智慧財產權保護，例如將表示多媒體版權的浮水印嵌入至多媒體資料中，可以驗證所有權(Authentic Ownership)或者保護資料不被非法複製與散播。

隨著時代與科技的進步，資料經過數位化後，更加容易複製、儲存或透過網路傳輸。現今的資訊隱藏技術，已經可以將秘密資訊隱藏在任何經過數位化後的資料，例如電子文件、影像、音訊、視訊、網路封包、軟體、檔案系統……等等③。

其中數位影像資訊隱藏是現今網際網路上最常應用，也是學術界最常研究的項目之一。主要的原因是全球資訊網(World Wide Web, WWW)的風行與數位輸出入設備的普遍，另一個原因是影像資訊隱藏效果的優劣，除了可由量化數據評估外，更可由人眼視覺直接判斷，因此較爲實用。

目前網際網路上常見的數位影像檔案格式有BMP、GIF、JPEG、TIFF、PCX等等，其中JPEG(Joint Photographic Experts Group)是由國際標準組織與國際電工委員會(ISO/IEC)在1994年所制訂的標準，由於其爲失眞型(lossy)的影像壓縮格式，可以將原本極大的資料量壓縮成較小的容量，而不至於對影像品質造成重大的影響，因此被廣泛的使用在網頁、數位相機……等需要透過網路傳輸或降低儲存空間的應用上。

JPEG2000同樣是由國際標準組織與國際電工委員會在2000年所制訂的新一代影像標準④，具有比JPEG更佳的壓縮效率與影像品質，同時也增加了對未來各種新興影像應用的支援，預料未來將成爲數位影像格式的主流。

本文將探討如何在數位影像中進行藏密，並深入研究新一代的影像標準JPEG2000的壓縮與編碼方式，進一步探討如何有效地在JPEG2000影像中進行資訊隱藏。

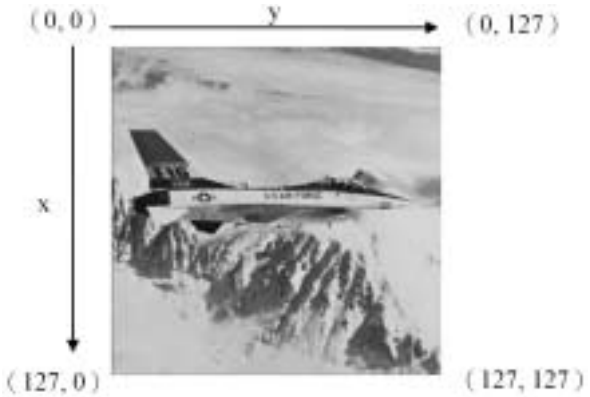
影像藏密技術

影像是傳達訊息非常直接又有效的方式，千言萬語形容女子的美貌，不如一張佳人的相片來得傳神。影像對人類的感官影響程度，不言而喻。我們生活週邊的類比影像經過數位化處理後即成爲電腦可以處理的數位影像(Digital Image)。數位影像常見的應用範疇，除了個人或家庭應用頻繁的網頁設計與數位相機外，還可提供醫學領域協助醫學診斷、太空衛星遙測進行科學研究、工業設備進行品質檢測、影像身份辨識、建築裝潢輔助設計、影像電話通訊……等等各種應用。而這許多新興的應用多半是伴隨著電腦功能的進步與網路通訊的便利而來。

一張數位影像在電腦上可以用一個二維(2-dimesion)的矩陣來表示，假設這個矩陣

③ N. F. Johnson, Z. Duric, and S. Jajodia, "Information hiding: steganography and watermarking-attacks and countermeasures," Kluwer Academic Publishers, 2001.

④ http://www.jpeg.org/jpeg2000/index.html.



圖二　數位影像示意圖 (作者繪製)

爲A(x_i, y_i),0≦x_i≦X,0≦y_i≦Y，其中X表示這張影像垂直方向的高度(height)，Y代表水平方向的寬度(weight)，A(x_i, y_i)代表影像中某一座標點的值。如圖二所示：

一張128×128的灰階(Gray-level)影像，整張影像是由16,384個(128×128=16,384)稱作像素(pixel)的點所構成，每個像素用8個位元(bit)來表示該點的光度或亮度值，共有256個灰階值。影像的容量爲128×128/1024×8/8=16 KBs(Kilo Bytes)。而同樣大小的彩色數位影像，每個像素使用24個位元，其中三個8個位元分別表示紅、綠、藍三種原色(RGB)的色階變化，影像的容量則爲128×128/1024×24/8=48 KBs。

數位影像通常爲了降低儲存成本或提高網路傳輸效率，會對影像進行壓縮處理，以減少其資料量。依據不同的應用，影像可以進行不同程度的壓縮，例如醫學用影像或衛星影像，對於影像內容要求十分嚴格，不容許有失眞的情況產生，可以使用無失眞性壓縮；而若是一般網頁影像或數位相機影像，因爲人眼無法明顯感受影像間細微的差異，因此可以在合理的範圍內使用失眞性壓縮加以處理。

影像壓縮最直接的方法就是將影像本身的冗餘(redundancy)部分去除。常見的影像冗餘性有⑤：

一、像素間冗餘性(Interpixel Redundancy)

影像相近像素之間所存在的信號關連性。

二、視覺冗餘性(Psychovisual Redundancy)

人眼對於複雜區域(紋理度較高)的改變較不敏感，對於平滑區域的改變則較爲敏感。另外，人眼對於相近的顏色也容易產生模糊或遮罩(masking)的情形。

三、編碼冗餘性(Coding Redundancy)

這是指以熵(entropy)編碼的概念，以最有效率的編碼方式來表現數位影像的資料。常見編碼方法如可變長度編碼(Variable Length Coding)、RLC編碼(Run Length Coding, RLC)、霍夫曼編碼(Huffman Coding)或算術編碼(Arithmetic Coding)。

值得注意的是一般影像藏密技術的概念恰巧與影像壓縮對於冗餘性資料的處理方式相反。影像壓縮爲了提高壓縮比，會盡可能的將冗餘的資料減少；而影像藏密技術則是找出影像資料中冗餘的部分，將秘密資訊隱藏在其中。因此影像藏密技術必須避免將所有資料都藏入影像冗餘資料內，以免在影像經過壓縮後，將所藏入的秘密資訊破壞殆盡。

目前常見的數位影像藏密技術可概略分爲空間域(Space Domain)及頻率域(Frequency Domain)兩類方法。

一、空間域方法

空間域方法指的是直接修改影像像素以

⑤ 繆紹綱，數位影像處理－活用Matlab，(台北：全華科技圖書股份有限公司，2000年)。

達到資訊隱藏的目的。常見的空間域資訊隱藏技術有最低位元取代法(Least Significant Bit, LSB)⑥、調色盤法(palette)、擬亂排列法(Pseudorandom Permutation)、向量量化法(Vector Quantization, VQ)⑦、補丁法(patch-work)⑧等各種方法。其中最常見也最基本的方法是最低位元取代法。舉例而言，某個灰階影像的像素值以二進位表示如下：

10011000；

由左至右分別表示高位元至低位元，其像素值爲$1\times2^7+0\times2^6+0\times2^5+1\times2^4+1\times2^3+0\times2^2+0\times2^1+0\times2^0=152$。假設將最低位元0修改爲1，則像素值將改變爲：

1001100**1**=153。

對於人類肉眼而言，灰階值的些微改變並不容易被發覺，因此可以將秘密訊息以改變最低位元的方式來藏入。當需要藏入的容量愈高時，可以選擇不只一個位元藏入，例如：

10011**01**=155；

10011**11**=159；

分別藏入了兩個位元及三個位元，其像素值隨著藏入位元數量的增加會與原本的像素值差異愈大，也因此較爲被肉眼發覺。一般而言，大多建議進行LSB藏密方法時不要在單一像素異動超過最後4個位元，以確保其不可察覺性。

二頻率域方法

另一類方法是先將影像進行轉換(transform)，在頻率域中對轉換後的影像係數(coefficients)進行藏密後，再將影像反轉換回空間域。影像經過轉換後，除了能提高影像壓縮效率外，對於影像內容的特性(如能量、邊緣、紋理度等)也較易掌控，因此爲許多失眞型的影像標準所採用。常見的影像轉換方法有快速傅立葉轉換(Fast Fourier Transform, FFT)、離散餘弦轉換(Discrete Cosine Transform, DCT)、離散小波轉換(Discrete Wavelet Transform, DWT)等。目前常見的JPEG是使用DCT，而本文主要討論的JPEG2000則是採用DWT。

離散小波轉換將影像先以水平垂直兩個方向作高低通濾波，分別產生LL、LH、HL、HH四個子頻帶(subband)，其中LL代表影像低頻的部分，LH與HL代表影像中頻的部分，而HH代表影像高頻的部分。LL可以再接著執行離散小波轉換，產生下一階(level)的子頻帶，如圖三所示：

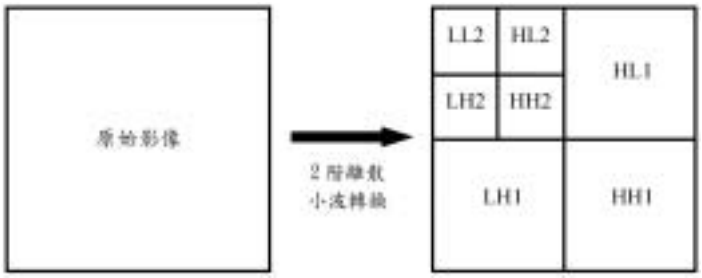
爲了避免影像經過藏密之後，造成內容過於明顯的差異，資訊隱藏技術大多選取影像中頻的部分，而避免藏入低頻或高頻的部分。更動低頻係數容易對影像內容產生明顯的影響，造成人眼可以輕易的感受到差異；至於高頻係數的部分在影像進行壓縮時容易被忽略，造成資訊的遺失，因此影像的中頻係數是較爲適當的影像藏密選擇處。

影像藏密技術，如果以高容量爲需求，一般仍會以空間域方法爲主，因爲其優點是

⑥ C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," IEEE Journal on Select Areas in Communications, vol. 16, no. 4, May 1998, pp. 525-539.

⑦ T.-S. Chen, C.-C. Chang, and M. S. Hwang, "Virtual image cryptosystem based upon vector quantization," IEEE Transactions on Image Processing, vol. 7, no. 10, October. 1998, pp.1485-1488.

⑧ W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM System Journal, vol. 35, no. 3 and 4, 1996, pp. 313-336.



圖三　影像經過2階離散小波轉換後各子頻帶分布情形 (作者繪製)

計算快速，可藏容量也較大，但相對的必須面對影像壓縮可能造成的破壞；而若需求是以強固性爲考量，則大多會採用頻率域方法，因爲頻率域方法，可以有效的消除像素間的冗餘性，也更容易分析影像的特性，找出最適合藏密的位置，唯一的缺點就是需要較大的計算成本。

JPEG2000影像壓縮標準

JPEG是國際標準組織與國際電工委員會(ISO/IEC)在1994年所共同提出的壓縮標準。JPEG利用離散餘弦轉換將影像資料中較不重要的部分去除，僅保留重要的資訊，可以同時提高壓縮率與確保影像的品質，是目前最受歡迎的影像檔案格式，也是數位相機所採用的影像格式。

目前已知JPEG對靜態的全彩與灰階影像有很好的壓縮效果，隨著多媒體與網路的快速發展，當人們開始對影像品質與影像功能有更多的要求時JPEG便開始顯現不足之處，例如：壓縮至0.25bpp(Bit Per Pixel)以下時，影像品質不佳、無法有效滿足醫學影像之高品質要求、無法支援大於64000×64000像素的圖像、對圖文混和型影像壓縮的效能不佳等。

ISO/IEC自1997年3月開始籌劃新一代靜態影像的壓縮標準，歷經多項提案與測試之後，於2000年完成基本的核心編碼架構，並正式將其命名爲JPEG2000⑨。新一代的JPEG2000與JPEG之間有幾項技術上的差異，如表一所示。JPEG2000除了有比JPEG更佳的壓縮效率與影像壓縮品質，也增加了對於各種新興的影像應用功能。

JPEG2000的特點如下⑩ ⑪ ⑫：

一更高的壓縮比與高影像壓縮品質。

二採用離散小波轉換做爲影像轉換的核心技術。

三同時支援失眞性與無失眞性壓縮。

四支援大型影像，最大至232×232大小。

五支援依影像品質或解析度漸進式傳輸(Progressive Transmission)。

六支援影像與文件混和壓縮。

七支援感興趣區域(Region Of Interest, ROI)。

表一　JPEG與JPEG2000主要差異比較表 (作者繪製)

項　　目	JPEG	JPEG2000
影像轉換方法	離散餘弦轉換	離散小波轉換
掃描方法	Z字型掃描(Zigzag)	位元平面掃描
熵編碼方式	霍夫曼編碼	算術編碼

⑨ ISO/IEC 15444-1: Information technology-JPEG2000 image coding system Part 1: core coding system, 2000.

⑩ 戴顯權，陳政一，JPEG2000，(高雄：紳藍出版社，2002年)。

⑪ 吳炳飛等，JPEG2000影像壓縮技術，(台北：全華科技圖書股份有限公司，2003年)。

⑫ D. Taubman and M. W. Marcellin, "JPEG2000: image compression fundamentals, standards and practice," Kluwer Academic Publishers, 2001.

圖四　JPEG與JPEG2000影像品質比較圖 (作者繪製)

八支援隨機存取(Random Access)特定區域的影像。

九較佳的錯誤復原力(Error Resilience)。

在相同的視覺品質之下，JPEG2000的平均壓縮比較JPEG高20%，在高壓縮比情況下，JPEG2000的視覺效果明顯優於JPEG，如圖四所示，也不再出現JPEG在高壓縮比容易產生的區塊效應(Block Artifact)。

目前完整的JPEG2000共包含11個部分⑬，如表二所示。其中Part 7原本是關於硬體實現的相關規範，已經終止規範。JPEG2000當初完成的標準只包含Part 1至Part 6, ISO/IEC從2001年為了使JPEG2000能更符合未來多樣化的應用需求，開始擴充Part 8至Part 12，目前仍在持續進行各項提案討論與測試。其中值得注意的是Part 8部分(JPSEC)提供影像安全的支援性，包括確保影像完整性、影像使用權限控制與著作財產權保護等，都將列入其標準支援的功能。

JPEG2000編碼與解碼流程

JPEG2000標準的編碼與解碼流程如圖五所示。原始影像首先經過前置處理後進行離散小波轉換處理，轉換後的影像係數再透過量化處理，交由EBCOT編碼器進行最佳化的編碼。在解碼時，只需將整個編碼流程反過來即可。

表二　JPEG2000架構一覽表 (作者繪製)

Part	主題	內容
1	核心編碼系統 (Core Coding System)	基本編碼與解碼方法。
2	延伸功能 (extension)	提供除了基本編碼以外的特殊功能。
3	動態 JPEG2000 (Motion JPEG2000)	可將數張 JPEG2000 影像集合成具動畫效果的連續影像。
4	標準化測試 (Compliance Testing)	測試 JPEG2000 編碼的複雜度與正確性判斷。
5	參考軟體 (Reference Software)	提供基本功能的測試參考軟體，供作測試。
6	圖文混和檔案格式 (Compound Image File Format)	針對圖文混和型的影像，將文字與影像以最佳狀態進行編碼。
7	略	略
8	JPSEC 安全性 (JPSEC Secure JPEG2000)	增加 JPEG2000 本身對加密、數位浮水印與權限控制的支援。
9	JPIP 互動工具介面與協定 (JPIP Interactivity Tools APIs and Protocols)	增加 JPEG2000 在不同網路與應用上的傳輸效能。
10	JP3D 3D 與浮點資料 (3D and Floating Point Data)	提供 JPEG2000 對 3D 影像更有效的支援。
11	JPWL 無線應用 (wireless)	明確規範 JPEG2000 在無線應用上可能的限制與條件。
12	ISO 國際標準媒體檔案格式 (ISO Based Media File Format)	增加 JPEG2000 與其他 ISO 的標準如 MPEG 的相容性，同時考慮支援未來 MPEG-21 格式。

⑬ R. Clark, "Taking image compression into the new millennium JPEG2000, a new standard to enrich imaging applications," ISO Bulletin, vol. 34, no. 2, February. 2003, pp. 17-19.

圖五　JPEG2000編碼與解碼流程示意圖 (圖片取材自⑳)

一前置處理階段

JPEG2000的特色之一，是對於大型影像的支援，如果影像尺寸較大，前置處理階段，會分割成較小的區塊，再分別處理。如果是彩色影像，則接著進行色彩轉換。前置處理階段中最重要的工作，是將影像的像素值作位移，以利後續的編碼。假設某個影像其像素值範圍在[0, 2^{N-1}]，其中N表示每個像素點用N個位元來表示，則必須將每個像素值範圍減去2^{N-1}，使得新的係數值範圍分佈在[-2^{N-1}, $2^{N-1}-1$]。例如8位元的灰階影像，原本的像素值範圍介於0~255之間，位移之後範圍將改介於-128~127之間。

二離散小波轉換

前置處理後，JPEG2000接著進行影像轉換的流程。JPEG2000所採用的離散小波轉換有9/7與5/3⑭兩種，其中9/7轉換爲實數模式(Real Mode)，是以浮點數運算，屬於不可逆的轉換，用來支援失眞性壓縮；而5/3轉換爲整數模式(Integer Mode)，是以整數運算，屬於可逆的轉換，能同時支援失眞性與無失眞性壓縮。JPEG2000的失眞性壓縮大多採用9/7轉換。

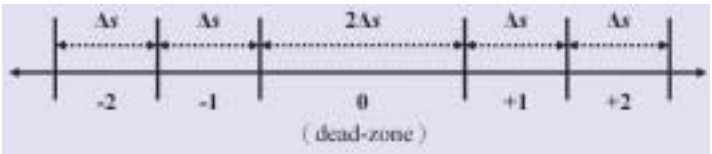
三量化

經過JPEG2000離散小波轉換之後，接著即進行量化階段。量化階段大致是根據人類視覺的特性作調整，也由於量化會將影像的小波係數作微調，因此會造成些微的失眞情況。比較特別的是JPEG2000所採用的均勻量化器在0附近的量化區間(通常稱爲死域，dead-zone)是其他區間的兩倍，如圖六所示。

這種作法的原因是經證明發現，具備拉普拉斯(Laplacian)機率分布的訊號，此種量化方式具有最佳的量化品質⑮。另外亦可以達成支援JPEG2000的漸進式傳輸功能與更精確的位元率控制(Rate Control)，以期影像能在目標位元率之下達到最佳化的影像品質。

四EBCOT編碼

JPEG2000擁有極佳的壓縮品質，絕大部分的功勞要歸功於EBCOT編碼演算法(Embedded Block Code With Optimal Truncation)⑯。EBCOT基本上是兩階段編碼器(2-tier Encoder)，第一階段先將影像子頻帶細分成相同大小的編碼區塊(Code Block，一般是64×64)，各個編碼區塊再獨立進行



圖六　JPEG2000量化區間示意圖 (圖片取材自⑫)

⑭ 同註⑰。
⑮ Ibid., 12.
⑯ D. Taubman, "High performance scalable image compression," IEEE Transactions on Image Processing, vol. 9, no. 7, July 2000, pp. 1158-1170.

編碼，產生前文(context)並利用全文(MQ)編碼器進行算術編碼產生位元串流；接著第二階段將這些位元串流作最佳化位元率與失眞度控制(Rate-distortion Optimization)並進行編碼串流(code-stream)封裝作業，以產生檔案所需的封包(如圖七)。

EBCOT採用位元平面(bit-plane)方式對影像編碼，編碼之前每個編碼區塊會先經過位元平面分解(decomposition)的程序，將影像區分成符號平面(Sign Bit-plane)與數值平面(Magnitude Bit-plane)。例如一張8位元的灰階影像進行EBCOT編碼時，影像資料會區分成8個位元平面，第1個位元平面用來代表符號，剩餘的7個位元平面用來代表數值，如圖八所示。

編碼時EBCOT會從最上面的位元平面(Most Significant Bit-plane, MSB)依序編碼至最低位元平面(Least Significant Bit-plane,LSB)，產生的位元串流，接著再依據期望位元率，進行最佳化的位元率控制。

EBCOT在位元率控制利用了分層(layer)的觀念⑰，將影像資料的位元串流依重要性分層儲存，分層的優點就是對於影像品質或解析度可以保持最佳化，也能支援漸進式的傳輸功能。

JPEG2000資訊隱藏技術

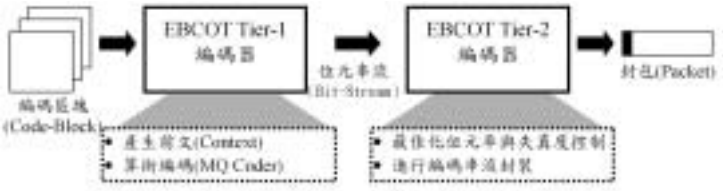
許多影像資訊隱藏技術例如展頻技術(spread-spectrum)⑱、亂數攪亂技術(Pseudo-random Permutation)、同構技術(automorphism)⑲等等，在應用到各種不同的影像格式時，都必須考慮到影像本身的特性。JPEG2000影像資訊隱藏技術，一般會考慮在JPEG2000標準編碼程序中的離散小波轉換、量化及EBCOT編碼等三個階段進行。

一、離散小波轉換階段

離散小波轉換對於一般訊號雜訊的抵抗性較佳，影像空間與頻率之間的對應關係也較易掌握，並且因爲其較接近人眼視覺模式(Human Visual System, HVS)，因此在壓縮時能保持較佳的視覺品質。在此階段的資訊隱藏技術，大多利用展頻技術或多重嵌入的技術，以提高藏密資訊的強固性。

二、量化階段

量化通常可以降低影像視



圖七　EBCOT編碼流程的示意圖 (作者繪製)

圖八　影像位元平面示意圖 (作者繪製)

⑰ Ibid., 12.

⑱ I. J. Cox, J. Kilian, T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, December 1997, pp. 1673-1687.

⑲ G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking," Proceedings of the ICIP, vol. 2, September 1996, pp.237-240.

覺冗餘性，增加影像壓縮的效能，而一般資訊隱藏技術常利用不同的量化區間作爲藏密的位置。JPEG2000量化階段，通常因爲不同程度的壓縮，會造成不同比例的資訊遺失，若在此階段藏入秘密資訊，則秘密資訊通常也會因壓縮而被破壞。因此除非影像進行無失眞壓縮，能保有所有資訊，否則此階段並不適合做JPEG2000資訊隱藏。

三EBCOT編碼階段

EBCOT編碼階段是JPEG2000中最重要的部分，其中第二階段的編碼，主要負責做最佳化位元率的控制，影像的資料會在這個階段因爲不同的壓縮比率而有不同程度的遺失，因此選擇在EBCOT第二階段之後才做資訊隱藏，可以確保藏密資訊最爲強固，但相對的缺點是較易造成影像的失眞，因此可藏入的容量較少。

2001年，Su等學者考慮影像壓縮與JPEG2000編碼的不同特性，選擇能同時抵抗影像壓縮又能確保所藏入的秘密資訊⑳。本方法選擇代表影像重要資訊的重要係數(Significant Coefficients)作爲藏入的對象；因爲影像在壓縮時，重要係數變動的機率不高。本方法利用一組密鑰(Secret Key)產生與EBCOT編碼區塊係數個數相同的隨機雜訊序列(Random Noise Sequence)來當作要藏入的秘密資訊，接著在編碼區塊中選擇一個係數門檻值(Threshold Value)，選擇大於該門檻值的係數藏入秘密資訊。這個方法對於一般訊號的雜訊均能有效的判定出是否有藏入特定的秘密資訊，但在檢驗時是採用係數之間相關性(correlation)作判斷依據，並非將實際的隱藏資訊取出；因此本方法較不適合用來作秘密資訊的傳遞，而較適合應用在數位浮水印或影像權益保障方面。

2001年，Grosbios等學者考慮在實作EBCOT編碼時，每個位元平面間的位元串流，會再多加兩個位元組(0xFFFF)以作爲區隔；因爲這些位元組與影像本身的內容無關，因此可以當作藏入秘密資訊的位置㉑。該方法先將欲傳送的秘密資訊以安全雜湊函數(Secure Hash Function,SHA)或MD4、MD5等雜湊函數產生訊息摘要(Message Digest)，再將這些資訊嵌入到各個位元組中。但是該方法的限制是可藏入的資訊容量不大，如果影像壓縮比極高，可能沒有足夠的空間作訊息的嵌入，因此該方法較適合作爲影像鑑別(authentication)的應用。

2002年，Noda等學者結合了JPEG2000的編碼流程與BPCS(Bit Plane Complexity Segment)的藏密技術，提出了一套適合JPEG2000作大量訊息傳遞的方法㉒。所謂的BPCS藏密方法，同樣也是將影像先以位元平面的方式分解，再依據每個位元平面的影像複雜度，將秘密資訊隱藏在影像紋理度較高的複雜區域，以避開人眼的察覺。

---

⑳ P.-C. Su, H.-J. Wang, and C.-C. Jay Kuo, "An integrated approach to image watermarking and JPEG 2000 compression," Journal of VLSI Signal Processing, vol. 27, 2001, pp.35-53.

㉑ R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG2000 compressed domain," Proceedings of the SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV, vol. 4472, 2001, pp.95-104.

㉒ H. Noda, J. Spaulding, M. N. Shirazi, and E. Kawaguchi, "Application of bit-plane decomposition steganography to JPEG2000 encoded Images," IEEE Signal Processing Letters, vol. 9, no. 12, December 2002, pp.410-413.

BPCS位元平面的藏密方式，恰巧符合EBCOT編碼的方式，因此該方法巧妙的利用EBCOT解碼時，才利用BPCS方法，選擇適合的位置藏入秘密資訊後，再一次的進行EBCOT編碼。這個方法具有高容量的優點，但卻因爲需要進行兩次的EBCOT編碼，執行效能較不佳。

2004年，Liu等學者針對EBCOT位元率控制的方式，選擇對影像品質影響較小的係數藏入秘密資訊，能有效降低因爲壓縮而造成藏密資訊被破壞的情形，並能完整的取出秘密資訊㉓。該方法爲了增加藏密容量及強固性，同時選擇影像低頻與中頻的部分，選擇具有特定形式的係數藏入秘密資訊，可以有效降低因爲係數改變所引起的影像失眞程度。因此該方法適用於目前網際網路傳輸頻寬有限的環境，可以在影像高壓縮比的情況下，保有所隱藏的秘密資訊。

上述各方法之間的比較如表三，由表三可以看出不同的方法其優缺點也不同，因此JPEG2000的資訊隱藏技術目前仍沒有一個完美的方法，必須依據不同的應用作調整，以符合實際的應用。

表三　JPEG2000資訊隱藏技術比較表 (作者繪製)

提出學者	執行階段	優點	缺點	應用範疇
Su	EBCOT	強固性高 計算快速	無法完整取出 藏密資訊	數位浮水印
Grosbios	EBCOT	安全性高	容量太小	影像鑑別
Noda	EBCOT	容量高	計算成本高	影像藏密
Liu	DWT+EBCOT	視覺效果佳	僅益於壓縮效果	數位浮水印

結論

資訊隱藏概念與軍事一直保有密切的關係，從中國古書「孫子兵法」、「三十六計」中可以發現不少類似這類欺敵致勝的例子。現今雖已是數位化的時代，但戰爭的威脅從未消失。當我們在享受網際網路與數位化快速便利的同時，日常生活周遭的電子文字、影像、音訊、視訊，未來將被廣泛利用在各種軍事、商業或政治等資訊隱藏用途上。因此對於各種資訊隱藏技術的研究發展，甚或於偵測與反制的技術，將是刻不容緩的重要研究課題。

JPEG2000是新一代數位影像的標準，現今諸如Photoshop、Photoimpact 8、IrfanViewer等知名影像處理或秀圖軟體，已經可以支援JPEG2000的影像格式；IE瀏覽器也具備有JPEG2000的外掛模組，在商業及個人等各種應用JPEG2000將逐漸普及。應用於JPEG2000的資訊隱藏技術方興未艾，現正是我們注入心力研究的最佳時機。

譯者簡介

周兆龍上尉，中正理工學院資訊系87年班、國防大學中正理工學院電子工程研究所93年班碩士。曾任電腦硬體工程官，現任空軍桃園基地指揮部管理資訊科程式設計官。

婁德權上校，中正理工學院電機系76年班、國立中山大學電研所碩士、國立中正大學資工所博士。曾任陸戰隊排長、陸戰師裝載官、助教、講師、副教授。現任國防大學中正理工學院電機系教授兼電算中心主任。

㉓ J.-L. Liu, D.-C. Lou, M.-C. Chang, C.-L. Chou, and C.-C. Pan, "A JPEG 2000 compatible digital watermarking scheme," The IEEE International Conference on Multimedia and Expo (ICME'2004), 2004 (accepted).