高相容性 JPEG 2000 影像加密技術之研究

劉江龍
國防大學理工學院電機電子系
副教授
e-mail：chianglung.liu@gmail.com

吳正陽
中山科學研究院電子系統研究所
技佐
e-mail：ooggwu@gmail.com

摘要

本文提出一個高相容性的 JPEG 2000 影像加密技術，其為一輔助工具，可利用密碼學工具或已在 JPSEC 註冊機構登錄之加密技術來對 JPEG 2000 封包進行加密，並輸出符合 JPSEC 標準之編碼串流，而加密後 JPEG 2000 編碼串流則可同時被標準的 JPEG 2000 解碼器所正確解碼。實驗結果顯示，在加密過程中所產生的額外解密資訊可以被嵌入在主檔頭中而不會造成標準解碼器解碼的錯誤。而加密後的 JPSEC 編碼串流則可被符合 JPEG 2000 Part 1 標準解碼器正確解碼，也同時可被支援 JPSEC 的解碼器正確解碼及解密，亦即本文所提出的加密技術可以符合高相容性的需求。因此，本文所提出的加密技術具有實用性及安全性。

關鍵詞：JPEG2000、JPSEC、封包加密。

Abstract

This paper proposes a high-compatibility JPEG 2000 encryption scheme. The proposed scheme is a complementary tool which can take advantages of cryptographic or registered encryption tools to encrypt JPEG 2000 packets and output a JPSEC compliant codestream. Moreover, the encrypted JPEG 2000 codestream can also be exactly decoded by a standard JPEG 2000 decoder. Experimental results show that the extra decryption information generated in the encryption process can be embedded in the main header without causing decoding failure. The experimental results also show that the encrypted JPSEC codestream can be correctly decoded by JPEG 2000 Part 1 compliant decoder and decrypted by JPSEC compliant decoders. That is, the proposed encryption scheme can meet the high-compatibility requirement.

Keywords: JPEG2000, JPSEC, packet encryption.

1. 前言

由於網路及多媒體技術的進步，數位影像的使用在日常生活愈來愈普遍。也由於數位影像可以輕易透過網際網路獲得，數位影像的安全性備受關注。數位影像的安全問題包括著作權的保護、來源及內容的鑑別(Authentication)、影像內容的保護(Confidentiality)及存取控制(Access Control)等。一般而言，著作權的保護可以透過數位浮水印技術(Watermarking)[1]獲得解決。這類技術是藉由在被保護影像中嵌入不可見的私密資訊(稱為數位浮水印)而達成。當影像的所有權發生爭議時，則可以將隱含在影像中的浮水印取出以解決爭端。在另一方面，影像來源及內容的鑑別、影像內容的保護及存取控制則通常是結合密碼學技術來解決。

JPEG 2000 [2-4]為 ISO 和國際電工協會(IEC, International Electrotechnical Commission)於 2000 年 3 月所制定的新一代影像壓縮技術，其在低位元率下，提供了相當好的壓縮效果[3]。JPEG 2000 標準的目標之一是要能適應低頻寬、高雜訊的環境，及醫療圖像、電子圖書館、傳真、網際網路服務和保安等方面的應用。JPEG 2000 的特點整理如下[4]：

(1) 更高的壓縮比與高影像壓縮品質。
(2) 支援依影像品質或解析度之漸進式傳輸。
(3) 提供無失真(Lossless)及失真(Lossy)壓縮架構。
(4) 支援直接存取及處理檔案位元編碼(Bitstream)。
(5) 較佳的錯誤復原力(Error Resilience)。
(6) 支援感興趣區域(ROI, Region of Interest)。
(7) 支援大型影像，最大至 232x232 大小。
(8) 支援影像與文件混合壓縮。

為了保障 JPEG 2000 影像應用的安全，JPEG 2000 Part 8 (JPSEC)[5]致力於提供影像安全的支援，包括影像加密及影像鑑別等都已列入其標準支援的功能，經過學者多年熱烈的討論後，JPSEC 於 2006 年 6 月成為 ISO 標準

(ISO/IEC 15444-8)，且於 2007 年 4 月正式定版。因此，許多確保影像安全的技術均可整合至 JPEG 2000 格式中來保障數位影像的機密性(Confidentiality)及完整性(Integrity)。

由於 JPEG 2000 為新一代影像壓縮標準，因此已有許多針對 JPEG 2000 影像的加密技術被提出來[6-10]，其中可概分為針對 JPEG 2000 編碼串流(Codestreams)進行加密的技術[6-8]及在 JPEG 2000 影像的編碼過程中進行加密等兩類技術[9,10]。由於 JPEG 2000 編碼串流有特殊的編碼格式，如果加密的結果不能符合這個格式，將導致符合 JPEG 2000 Part 1 標準的解碼器無法正確解碼，也就是說，對符合 JPEG 2000 Part 1 標準的解碼器而言，將造成相容性的問題。因此，上述之加密技術均致力於提供相容性的加密服務。在 JPSEC 標準中已包括加密結果是否合乎 JPEG 2000 Part 1 標準的標示，此隱含符合 JPSEC 標準的加密工具不一定要提供符合 JPEG 2000 Part 1 標準的格式。例如在 JPSEC 附錄 B4[5]所使用封包內容(Packet Body)加密法(使用區塊加密法加密)，其在進行區塊填充後之加密結果就無法保證可以完全與符合 JPEG 2000 Part 1 解碼器相容，此同樣產生相容性問題。當加密後的結果產生相容性問題時，JPEG 2000 或 JPSEC 規範中的某些設計就可能無法百分之百保持 JPEG 2000 影像原有的特點或達到 JPSEC 安全規範所要達到的保護特性。

目前已有同時符合 JPEG 2000 Part 1 及 JPSEC 標準的加密工具被提出來，例如在 JPSEC 附錄 B5 之雙位元組(Two-Byte)加密法[5]及 Engel 等學者所提出之實作雙位元組加密法[11]等，然而 JPSEC 附錄 B5 只提出雙位元組加密之概念，並無實際加密演算法，而 Engel 等學者則是運用互斥或(XOR)法對封包內容實際進行雙位元組加解密，並制定五項加解密原則來推論 JPSEC 附錄 B5 之概念是可以解密的，因此，如果不是建構在 XOR 的特性(重覆二次 XOR 可以回復原始資料)之上，或許就必須修改加解密原則以達到此一結果，並且使用 XOR 當作的實際加密演算法，在安全性上應該是不夠完善的。而現有針對 JPEG 2000 Part 1 標準所發展的加密工具，若要符合 JPSEC 的標準，則需要針對 JPSEC 標準重新定義其加解密方法。為了能讓這些方法及爾後針對 JPEG 2000 Part 1 標準的新加密方法可以很方便的與 JPSEC 規範相結合，而又能不發生相容性的問題，本文提出一個新的 JPEG 2000 影像加密技術，其所產生之 JPSEC 編碼串流除了能被符合 JPSEC 規範的解碼器正確的解碼之外，也能同時被符合 JPEG 2000 Part 1 標準的解碼器所正確解碼，使得原始 JPEG 2000 影像在經過 JPSEC 的安全保護功能之後，仍能保有 JPEG 2000 影像的特點。我們特別定義此加密技術為高相容性加密技術，意謂其編碼結果可同時被上述兩種解碼器同時正確解碼。

在 JPSEC 規範中將加密方法稱為加密工具，主要分為二類：第一類為標準密碼學工具(Normative Tools)，第二類為非標準工具(Non-normative Tools)。標準工具是明確定義在規範中的工具，目的在達到影像的機密性(經由加密工具)及驗證資料來源的功能，而標準工具以外之加密工具則稱為非標準工具。非標準工具又可分為個人私有工具(Private Tools)及註冊機構(RA, Registration Authority)註冊工具(Registered Tools)兩類。JPSEC 註冊機構是讓使用者可以透過網路，將個人私有工具註冊，使得這些工具可以分享給其它使用者使用。因此，個人私有工具就是尚未在 JPSEC 註冊機構註冊的私有工具，僅侷限於研發者自己使用；而註冊機構註冊工具則表示已在 JPSEC 註冊機構註冊的私有工具。

本文所提出的加密技術定義為註冊機構註冊工具，主要是用以輔助其他加密工具達成高相容性的目的。透過本加密技術，使用者可以利用定義在 JPSEC 內之標準加密工具或已註冊工具來對 JPEG 2000 影像進行加密。因此，使用者可以自行選擇高安全強度的加密演算法進行加密，而加密後的影像則可同時被符合 JPSEC 或 JPEG 2000 Part 1 規範的解碼器所正確解碼。此外，在本技術的架構下，無論該加密演算法是串流加密(Stream Cipher)或是區塊加密法(Block Cipher)[12]，都無損加密之後的高相容性，突破以往只能固定使用區塊加密或是串流加密的方法。

為說明本文提出之技術，本文其餘各節安排如下：第 2 節介紹 JPSEC 語法；第 3 節提出符合 JPSEC 規範之高相容性加密技術；第 4 節為實驗結果；第 5 節為本文之結論。

2. JPSEC 語法

JPEG 2000 規範內定義了許多給解碼器識別之標記(Marker)。圖 2.1 分別表示 JPEG 2000 編碼串流與已進行機密性保護後的 JPSEC 編碼串流，並將這二個編碼串流進行比較。其中 SOC 標記為檔案起始標記，SIZ 標記指記錄此

影像之大小及相關參數區段，COD 標記為編碼型態參數區段，QCD 標記為量化值區段。由圖 2.1 可以得知，JPSEC 編碼串流多了 SEC 標記及區段，並且已對影像內容進行保護。

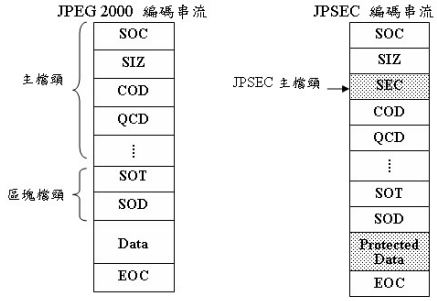

圖 2.1 JPEG 2000 與 JPSEC 編碼串流比較示意圖

SEC 標記是出現在主檔頭的標記，其值為 0xFF65，在這個標記之後則是 SEC 區段，是用來存放受保護文件的相關資訊。而 SEC 標記在主檔頭的位置必須接在 SIZ 區段之後，且 SEC 標記可以多次出現，表示使用多個 JPSEC 工具進行影像保護，如圖 2.2 所示。由圖 2.2 可以得知，在影像主檔頭中可以有許多的 SEC 標記及 SEC 區段，亦即 0xFF65 這個值在主檔頭中出現的次數即代表此影像的 SEC 標記個數。P_{SEC} 包含四個主要參數，如圖 2.3 所示。

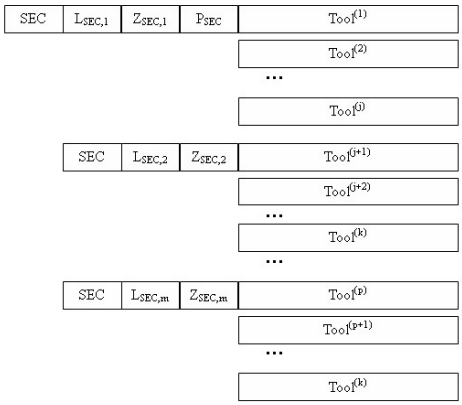

圖 2.2 多重 SEC 標記示意圖

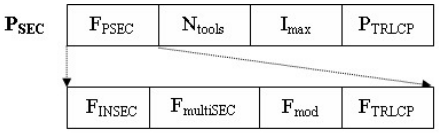

圖 2.3 P_{SEC} 語法

將圖 2.2 的 Tool 區段詳細展開後，其結構如圖 2.4 所示，共分為七個小區段。JPSEC 以安全性目的不同為主，將工具分為三種模式，每一種模式在 P_{ID} 區段會有不同的語法及表示意義，本文中僅使用解密模式。

圖 2.4 工具區段結構

在使用標準工具的情形下，ID 參數僅佔用 8 位元，主要是用來辨識此工具是屬於三種模式中的哪一種，如表 2.1 所示。

表 2.1 標準工具 ID 參數值

值	安全模式
0	保留
1	解密樣板模式(Decryption Template)
2	驗證樣板模式(Authentication Template)
3	雜湊樣板模式(Hash Template)
4	無使用工具
	其餘值保留給 ISO 使用

在使用非標準工具的情形下，ID 參數則定義為 ID_{RA} 參數，並且擴充如圖 2.5 所示。參數 $ID_{RA,id}$ 是用來辨識工具是屬於 JPSEC 註冊機構註冊工具或是由私有使用者所自訂之工具，而參數 $ID_{RA,ns}$ 為 ID_{RA} 的命名空間(Name Space)，由 JPSEC 註冊機構建立。

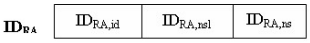

圖 2.5 ID_{RA} 參數區段

在使用非標準工具的情形下，P_{ID} 參數完全是由 JPSEC 註冊機構或私有工具使用者決定內部參數，故可以在此存放加密時所產生之額外資訊。而在使用標準工具的情形下，P_{ID} 參數如圖 2.6 所示，會再區分為 T_{ID}(Protection Method Template)、PD(Processing Domain)、G(Granularity)、V(Value List)等四個區段。其中只有 T_{ID} 參數依 ID 參數值而被區分為三種模式，但本文並未使用到驗證與雜湊模式。

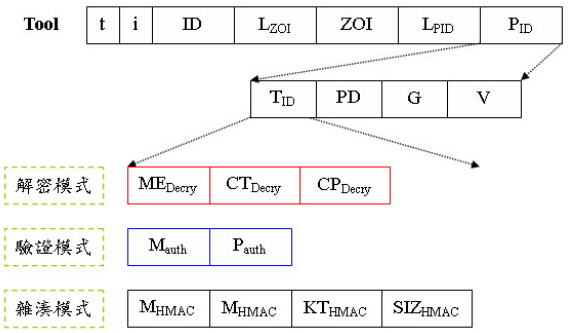

圖 2.6 JPSEC Tools 架構(使用標準工具)

3. 高相容性的加密技術

本節提出一高相容性的加密技術(以下簡稱為本技術)，其為一個已在 JPSEC 註冊機構註冊之工具，主要是用以輔助其他加密工具達成高相容性的目的。其所具備之功能如下：

(1) 透過本加密技術，使用者可以利用定義在 JPSEC 內之標準加密工具或已註冊工具來對 JPEG 2000 影像進行加密。

(2) 其所產生之 JPSEC 編碼串流除了能被符合 JPSEC 規範的解碼器正確的解碼之外，也能同時被符合 JPEG 2000 Part 1 標準的解碼器所正確解碼，此亦為高相容性之定義。

本技術係利用標準加密工具或 JPSEC 註冊之加密工具將封包內容加密，以達到影像在可調串流及轉碼安全上的保護。同時將加密過程中所產生的額外資訊放置於主檔頭，以利解碼器後續之解密。由於本技術採用標準 JPSEC 規範來存放額外資訊，故符合 JPSEC 規範之解碼器就可以直接對影像解碼。透過此加密技術，除可以保有使用標準工具加密時的高相容性，更可以直接使用在 JPSEC 註冊機構上已登錄之加密工具進行加密使用。

3.1 加解密流程

本技術可分為兩部分，一為加密部分，一為解密部分。加密流程如圖 3.1 所示，加密的來源可以為標準 JPEG 2000 編碼串流或是 JPSEC 編碼串流(符合 JPEG 2000 Part 8 標準)。因此，加密器會先嘗試讀取主檔頭及區塊檔頭資訊以解讀封包長度，若解讀成功，則繼續對封包內容進行加密，否則放棄加密。而加密工具的來源可以為標準之加密工具，或是已在 JPSEC 註冊機構上登錄之加密工具(以下稱為已註冊工具)。為了預防某些工具在加密後產生與 JPEG 2000 解碼器不相容之編碼串流，本技術利用「封包長度保存加密技術」進行封包內容調整，並將額外解密資訊嵌入編碼串流，最後輸出 JPSEC 編碼串流。

解密流程如圖 3.2 所示。進行解密時，由於該編碼串流符合 JPSEC 之規範，由符合 JPSEC 規範之解碼器先萃取解密資訊來還原加密影像。若解碼器判斷原加密工具屬於已註冊工具，則需先向 RA 下載解密資訊，透過該解密資訊取得解密工具，並由使用者輸入解密金鑰進行封包解密，最後輸出解密完成之 JPEG 2000 編碼串流。封包長度保存加密、額外資訊嵌入及封包解密分述於以下各節。

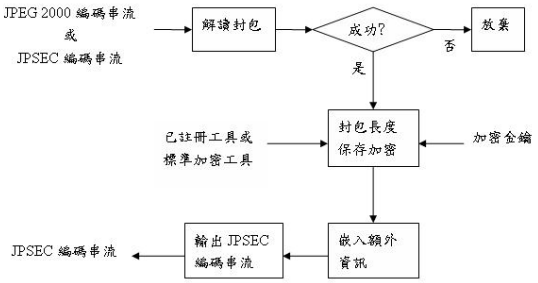

圖 3.1 本技術之加密流程

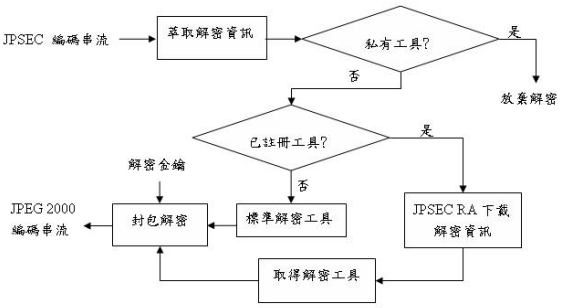

圖 3.2 本技術之解密流程

3.2 封包長度保存加密

本加密技術主要是針對 JPEG 2000 封包進行加密。若直接對封包進行密碼學加密，則可能會產生以下問題：

(1) 加密後封包長度可能比原始封包長，此狀況可能發生在採用 ECB、CBC 及 CTR 模式的區塊加密法[12]。

(2) 加密後封包的連續二個位元組可能超過 0xFF8F。

當發生上述二種問題時，都將導致標準 JPEG 2000 解碼器無法正常解碼，也就是造成相容性的問題。本技術提出「封包長度保存加密技術」來解決上述問題。換句話說，「封包長度保存加密」必須達到以下目的：

(1) 各封包加密後之長度保持不變。

(2) 封包加密後，其連續二位元組不超過 0xFF8F。

封包長度保存加密流程如圖 3.3 所示。雖然目前加密演算法(在 JPSEC 規範中稱為加密工具)相當多，但依加密方式則可以概分為區塊加密法以及串流加密法二種。使用本方法可以選擇使用已註冊加密工具或標準之加密工具(例如：AES 或 RSA)來進行加密。當加密器接收到封包內容，會先判斷是否為區塊加密法，若是，則判斷加密模式是否為 ECB、CBC 或 CTR，以及最後一個加密區塊是否有長度不足的情形，若是，則先進行封包填充，待填充後

再進行封包加密，否則直接進行封包加密，最後輸出加密後的封包。

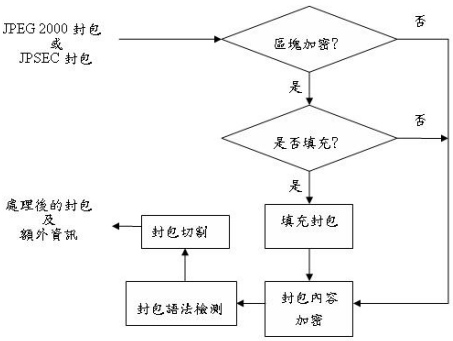

圖 3.3 封包長度保存加密流程圖

依據 JPEG 2000 Part 1 標準，在封包內容中，連續二個位元組不能存在十六進位 FF90 至 FFFF 之間的值，否則會造成解碼上的嚴重問題。換句話說，若加密後的封包內容出現上述的問題時，則很有可能會造成標準解碼器的混淆而不能成像，也就是產生與標準 JPEG 2000 解碼器不相容的問題。因此，為了與 JPEG 2000 Part 1 解碼器相容，上述加密後的封包在輸出編碼串流之前必須進行上述問題之過濾。本研究所採取的方法是在個別封包加密完成之後，對已加密的封包內容進行檢測，檢查是否存在連續二個位元組大於 0xFF8F 的值。若存在，則將第一個位元組改為 0xFE，並且記錄修改的索引位置作為額外資訊，並將索引位置儲存在 KVL(Kernel Value List)陣列中，KVL 陣列則會在下一階段以符合 JPSEC 語法嵌入在 SEC 區段內。

由於 KVL 陣列是記錄被修改為 0xFE 之 0xFF 位置，所以必須要先訂定記錄位置索引值的參考點。由於本加密方法並不會更動各封包的長度，因此本技術以個別封包檔頭位置作為參考點。亦即由該封包檔頭算起第 1 個位元組的索引值設定為 1，第 2 個位元組的索引值設定為 2，依此類推。若換至下一個封包，則索引值則換成以該封包檔頭作為索引值的參考點。為了方便解密，KVL 陣列一律採用 RBAS 結構記錄索引值，由於索引值不只一個，所以 KVL 陣列其實是一連串 RBAS 結構[5]所組成的 RBAS 序列。為能分辨各封包的索引值，KVL 陣列的第 1 個 RBAS 結構即為第 1 個封包內將 0xFF 修改為 0xFE 的個數，接著才是記錄這些修改位置的索引值。

舉例來說，假設某編碼串流有 2 個封包，在進行語法檢測之後，將 0xFF 值修改為 0xFE 之位置有三處，分別為從封包 1 檔頭算起第 118 及 12564 個位元組及封包 2 檔頭算起第 79889 個位元組。此三個索引值可分別以二進位表示為 1110110_2(118)，11000100010100_2(12564)及 10011100000010001_2(79889)，依 RBAS 序列建立原則，此 KVL 陣列如圖 3.4 所示。

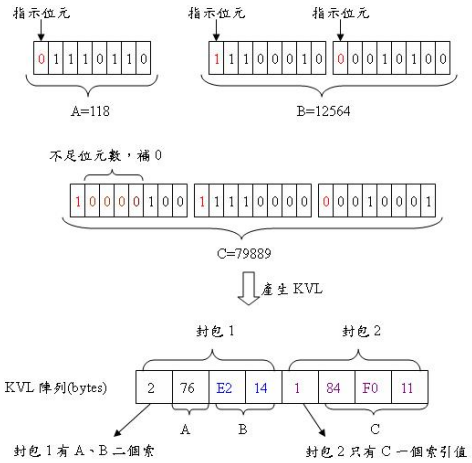

圖 3.4 KVL 陣列產生範例圖

假設現有 n 個已加密後的封包，各封包分別有 k_n 個位元組，則每個位元組必須要逐一進行語法檢測後才能建立 KVL 陣列。

為滿足加密後的封包長度不變，調整內容後的加密封包必須經過封包切割。亦即將加密後封包的最後一個區塊切割成二個部分，第一部分保留在該封包內，使得封包內容的長度保持不變；第二部分則為加密所產生之額外資訊，將其記錄於 PVL(Packet Value List)陣列內。此部分資訊則必須在下一階段以符合 JPSEC 語法嵌入在 SEC 區段內。

假設某 JPEG 2000 編碼串流共計有 n 個封包，a_i 為各個封包的最末區塊，令 X_i 表示用以填充 a_i 的明文，X_i 共有 L(X_i)位元組，$a_i||X_i$ 為封包 i 的最後加密區塊，Y_i 表示加密後區塊的末 L(X_i)位元組資料(L(Y_i)=L(X_i))。PVL 陣列則是合併所有封包之 Y_i 長度 L(Y_i)及 Y_i 值的結果，其產生流程如圖 3.5 所示，其中 L(Y_i)是使用 RBAS 結構來記錄。

綜合上述，個別封包保存加密步驟如下：

步驟 1. 依據選擇的加密工具及模式判斷封包是否需要填充，若是，則先對封包進行填充。

步驟 2. 依所選擇的加密工具及加密模式對封包內容進行加密。

步驟 3. 判斷加密後的封包中是否存在連續二個位元組大於 0xFF8F，若是，則修改

第一個位元組為 0xFE，並將修改數量及各修改位置索引值記錄於 KVL 陣列內。

步驟 4. 將超過原本封包長度的資料記於 PVL 陣列內。

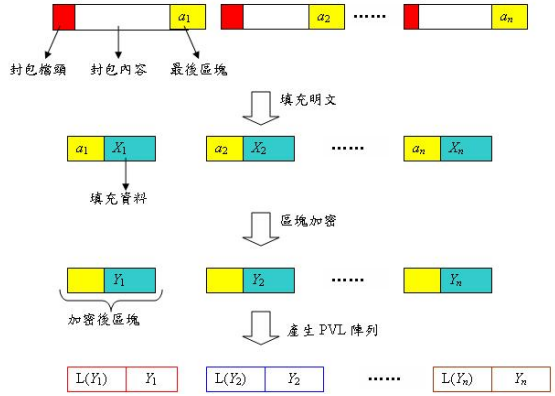

圖 3.5 PVL 陣列產生流程

3.3 額外資訊嵌入

為讓支援 JPSEC 之解碼器能對加密後的編碼串流進行解碼及解密，本技術在加密時將解密資訊及封包長度保存加密工具的相關資訊一併嵌入 SEC 區段。如第 2 節所述，若使用自訂工具，則 P_{ID} 參數必須由設計者自訂，而封包長度保存加密工具既為自訂工具，故需進行定義。假設封包長度保存加密工具已在 JPSEC RA 內登錄，且獲得編號為 ID_A，而 ID_B 則是用來表示標準工具所使用之 ID，或者是另一個使用者所提出之加密法在 RA 內之編號。封包長度保存加密工具之格式如圖 3.6 所示。

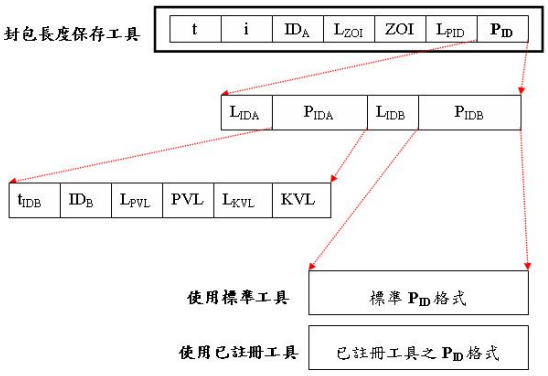

圖 3.6 封包長度保存工具架構

其中 P_{ID} 參數是可以包含已註冊工具或標準工具之 P_{ID} 參數，這也是能使用封包長度保存加密工具來囊括標準工具或是使用已註冊工具的原因。表 3.1 與表 3.2 則分別說明封包長度保存工具各區段參數所表示之意義。

表 3.1 封包長度保存工具 P_{ID} 參數表

參數	說明
L_{IDA}	為 P_{IDA} 的長度，使用 RBAS 結構，佔(8+8xn)位元
P_{IDA}	使用封包長度保存工具產生之額外資訊，參考表 3.2
L_{IDB}	為 P_{IDB} 的長度，使用 RBAS 結構，佔(8+8xn)位元
P_{IDB}	標準工具之 P_{ID} 格式或是已註冊工具之 P_{ID} 格式

表 3.2 封包長度保存工具 P_{IDA} 參數表

參數	說明
t_{IDB}	工具形式。位元值為 0 表示使用標準工具，位元值為 1 則表示使用已註冊工具。使用 FBAS 結構，佔 8 位元。
ID_B	使用標準工具請參考表 2.5，使用已註冊工具則 ID_B 則表示已註冊工具在 JPSEC RA 之註冊編號。此參數佔 32 位元
L_{PVL}	為 PVL 的長度，使用 RBAS 結構，佔(8+8xn)位元
PVL	儲存額外填充編碼串流之陣列
L_{KVL}	為 P_{IDB} 的長度，使用 RBAS 結構，佔(8+8xn)位元
KVL	儲存修改 0xFF 為 0xFE 的索引位置陣列，使用 RBAS 格式

3.4 封包解密

對於使用封包長度保存加密後的 JPSEC 編碼串流，由於已經將 PVL 與 KVL 二種資訊嵌入在 SEC 區段中，所以在解密前必須要能將該資訊萃取出來，以還原密文，接著才可以透過標準解密工具或經由 RA 下載已註冊工具進行解密。

封包解密流程如圖 3.7 所示，詳細解密步驟如下：

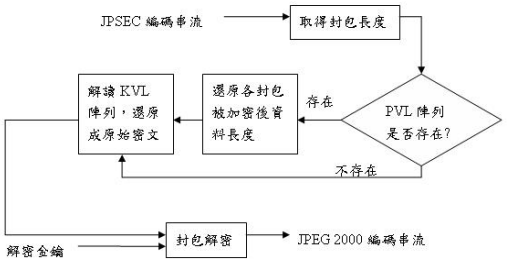

圖 3.7 封包解密流程圖

步驟 1. 解讀主檔頭，獲得並記錄各封包內容長度。

步驟 2. 解讀 PVL 陣列。若 PVL 陣列存在，則從 PVL 陣列取出 Y_i，還原至各封包 i 最末端。

步驟 3. 解讀 KVL 陣列，取出各索引值，並依索引值將 0xEF 資訊還原為 0xFF。

步驟 4. 由參數 t_{IDB} 及 ID_B 判斷是否使用已註冊工具加密，若是，則經由 RA 查詢 ID_B 並下載此工具解讀格式。

步驟 5. 配合使用之標準工具或已註冊工具及解密金鑰對密文進行解密。

步驟 6. 依據各封包長度資訊，取出合法的封包資料(即刪除各封包最末端填充之明文 X_n)，輸出 JPEG 2000 編碼串流。

4. 實驗結果與討論

4.1 實驗環境

(1)實驗平台：AMD Athlon 64 X2 Dual 3000+，2.51 GHz CPU、2 GB RAM 桌上型電腦。
(2)作業系統：Windows XP Professional。
(3)實驗工具：
a. Matlab 7.0 [14]：用以實作本文所提出之加密技術及 JPSEC 解碼器模擬程式。
b. IrfanView 4.22 Plugin [15]：可直接讀取 JPEG 2000 影像格式之免費看圖軟體，用以測試加密後之 JPSEC 編碼串流與 JPEG 2000 Part 1 解碼器之相容性。
(4)實驗圖像：將六張 256×256 的 8 位元灰階影像做 JPEG 2000 壓縮後再進行實驗，其 JPEG 2000 編碼參數如表 4.1 所示，影像如圖 4.1 所示。

表 4.1 實驗圖像編碼資訊

參數	值	說明
區塊	1	設定為 1 個區塊
小波階數 (WaveLevel)	3	進行 3 次小波轉換
小波轉換方式 (WaveType)	5/3	使用 5/3 濾波器做整數模式轉換，屬可逆轉換
分層(Layer)	3	將各編碼區塊均切割於 3 個分層之中
漸近模式	LRCP	層-解析度-元素-位置模式，即品質漸進模式，解碼端會將影像從粗糙的輪廓漸進式的改善成清晰的還原影像
編碼區塊	64×64	各編碼區塊為大小為 64×64 位元

4.2 實驗假設

(1) 編碼方式：由於本加密技術是對 JPEG 2000 封包內容進行加密，而 JPEG 2000 封包產生的方式並不會影響實驗結果，因此，本研究對各實驗圖像之 JPEG 2000 編串流採用同一套編碼方式。
(2) 加密方式：由於串流加密法在對封包內容加密時，並不會改變封包內容的長度，因此為了凸顯本方法之特性，本節的實驗均使用會改變封包長度的區塊加密法對不同 JPEG 2000 影像進行加密。
(3) 註冊編號：本研究假設在 JPSEC RA 內已登錄二個私有工具，編號 1 即為本文所提出之封包長度保存加密法，該加密法以封包為最小處理單位，以符合 JPEG 2000 各種漸進式模式；編號 2 則是已註冊之加密法。
(4) 標準工具：本研究採用 AES 演算法作為標準加密工具，同樣使用電子密碼本模式，採用 128 位元加密金鑰。

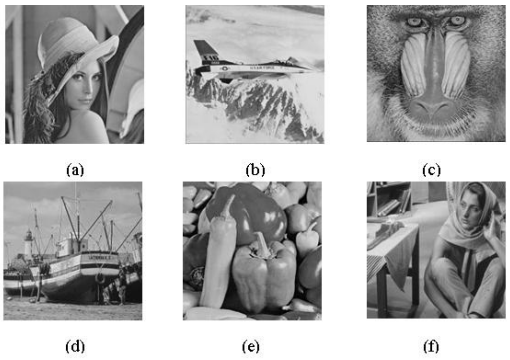

圖 4.1 本研究之實驗用圖

4.3 實驗結果

本實驗目的在於證明本文之加解密方法可使用標準工具對 JPEG 2000 編碼串流進行加密(相同結果可套用至其他已註冊工具)，其加密結果具有高相容性，即可同時被符合 JPEG 2000 Part 1 標準的解碼器及符合 JPSEC 標準的解碼器所正確解碼。為測試本加密技術之相容性，本研究透過上一節之實驗假設分別針對不同之實驗圖像進行 JPEG 2000 編碼串流之產生，並使用 IrfanView 看圖工具進行編碼串流之解碼，實驗結果分述於以下各小節。

4.3.1 JPEG 2000 Part 1 相容性測試

本實驗首先透過實驗假設的私密金鑰對各實驗用圖進行加密，並在尚未產生 SEC 區段解密資訊前將加密影像輸出。這些加密影像均經由封包長度保存加密法去呼叫標準加密工具(AES)來對各個封包進行有填充的區塊加密，並使用 KVL 陣列記錄不合法密文的修改處，同時使用 PVL 陣列記錄額外資訊長度，但尚未將此二種解密資訊嵌入至主檔頭，因此單純輸出符合 JPEG 2000 Part 1 之 JPEG 2000 編碼串流，圖 4.2 為利用 IrfanView 看圖工具分別對上述加密後之 JPEG 2000 編碼串流之解碼結果。

接著依照符合 JPSEC 規範之嵌入技術，將解密資訊 KVL 與 PVL 嵌入至加密後 JPEG 2000 編碼串流之主檔頭，再利用 IrfanView 進行解碼，其結果圖 4.3 所示。由圖 4.3 可以發現，在主檔頭嵌入各項解密資訊後，與尚未嵌入解密資訊時所解碼的影像是相同的，表示在主檔頭的 SEC 嵌入資訊並沒有影響到標準解碼器的解碼程序，亦即本加密技術可與標準解

碼器相容。

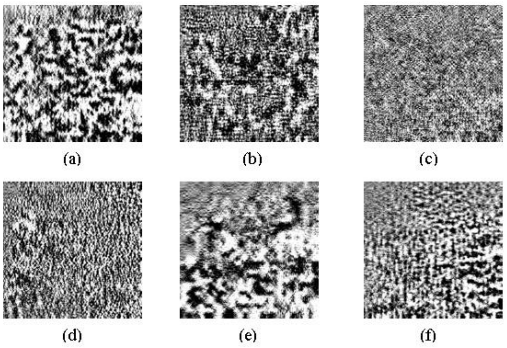

圖 4.2 使用標準 AES 工具加密後之 JPEG 2000 編碼串流影像

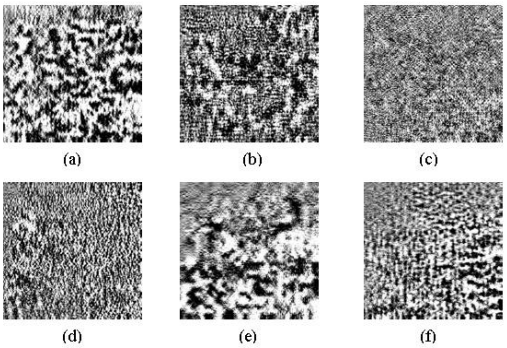

圖 4.3 使用標準 AES 工具加密後之 JPSEC 編碼串流影像

4.3.2 JPSEC 相容性測試

為測試本加密技術可與 JPSEC 標準解碼器相容，本實驗依照上一節之假設，在本技術的架構下，分別利用標準工具(AES)對各實驗圖檔的 JPEG 2000 編碼串流進行加密，並分別在主檔頭建立 SEC 區段。本研究同時撰寫符合 JPSEC 規範之解碼器模擬程式，並對加密後之 JPSEC 編碼串流進行解碼及解密。圖 4.4 為在未提供解密金鑰下所解碼的圖像，而在提供正確解密金鑰後則可得回原始之影像。由上述之實驗結果，利用本加密技術所產生的圖像可被符合 JPSEC 規範的解碼器正確解碼及解密，亦即可以與 JPSEC 解碼器相容。

4.4 實驗討論

本小節討論與本加密技術相關之實驗，包括相容性討論、額外資訊長度討論、執行效率討論及安全性討論等，分述於以下各小節。

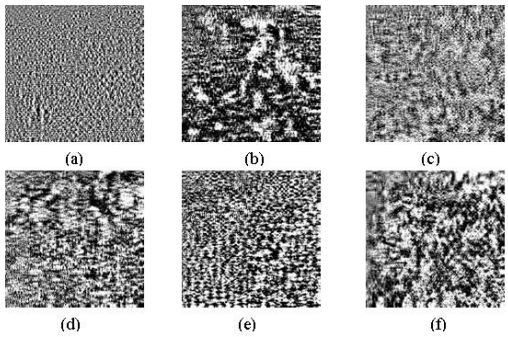

圖 4.4 在提供錯誤解密金鑰下，JPSEC 解碼器對使用標準加密工具之 JPSEC 編碼串流之解密結果

4.4.1 相容性討論

本小節主要在探討本技術與現有的 JPEG 2000 的加密工具對 JPEG 2000 Part 1 標準解碼器及 JPSEC 標準解碼器的相容性，同時對上述工具可使用的加密法進行比較。由於本技術為針對 JPEG 2000 編碼串流的加密技術，並非屬於在 JPEG 2000 的編碼過程進行加密的加密技術，所以探討比較的對象僅限於現有針對 JPEG 2000 編碼串流的加密技術。

表 4.2 為各 JPEG 2000 加密技術的相容性比較表，前四項技術為針對 JPEG 2000 Part 1 所提出，包括本技術之後四項技術則為針對 JPSEC 所提出。在加密方式方面，除了本技術外，其他加密技術只能使用區塊加密或串流加密；在 JPEG 2000 Part 1 語法符合方面，除 JPSEC 附錄 B4 的方法為針對 JPSEC 所提出，其加密後的結果不符合 JPEG 2000 Part 1 語法外，其餘的技術則完全符合 JPEG 2000 語法，可被 JPEG 2000 Part 1 解碼器所正確解碼，其中除了 Wu and Deng 所提出的技術及本技術外，其餘的技術則無法對封包內容完全加密；在 JPSEC 語法符合方面，由於前四項加密技術為針對 JPEG 2000 Part 1 所提出，其加密後的結果不符合 JPSEC 語法，而其餘四項技術則完全符合 JPSEC 語法，可被 JPSEC 解碼器所正確解碼，其中除本技術外，其餘技術均需要修改封包檔頭以符合 JPSEC 語法。

綜合上述，在相容性方面，本技術可適用於區塊加密法或串流加密法，也同時符合 JPEG 2000 語法及 JPSEC 語法，符合本技術所要求之高相容性的需求；此外，本技術可完全對封包內容加密，也不需要更改封包檔頭，因此，可結合其他加密技術來對 JPEG 2000 或 JPSEC 編碼串流進行加密。

表 4.2 各加密技術之相容性比較

加密技術	加密方式	Part 1 語法符合	封包內容完全加密	JPSEC 語法符合	修改封包檔頭
Wu and Ma [6]	串流加密	是	否	否	X
Wu and Deng [7]	串流加密	是	是	否	X
Dufaux. et al. [13]	串流加密	是	否	否	X
Yang. et al. [8]	串流加密	是	否	否	X
JPSEC 附錄 B4 [5]	區塊加密	否	否	是	是
JPSEC 附錄 B5 [5]	區塊加密	是	否	是	是
Engel D. et al. [11]	區塊加密	是	否	是	是
本技術	兩者均可	是	是	是	否

4.4.2 額外資訊長度討論

本加密技術透過在 SEC 區段嵌入額外資訊以輔助標準工具及已註冊工具達到相容性目的，因此，會額外增加 JPEG 2000 編碼串流的長度。本小節主要探討在主檔頭中所嵌入的額外解密資訊(PVL 陣列與 KVL 陣列)佔總影像大小的比例。表 4.3 為使用 AES 加密實驗圖像所產生額外資訊所佔總影像大小之百分比。由表 4.3 可發現，額外解密資訊只佔 JPEG 2000 編碼串流 0.429%至 0.655%之間，亦即對原壓縮率之影響不大。

表 4.3 AES 加密所產生之額外資訊

圖像	原始影像(位元組)	PVL(位元組)	KVL(位元組)	已加密影像(位元組)	(PVL+KVL)/已加密影像
Lena	35,767	88	102	36,024	0.527%
F16	36,675	78	131	36,952	0.566%
Baboon	50,403	126	178	50,775	0.599%
Boat	40,643	97	154	40,962	0.613%
Peppers	36,788	107	136	37,099	0.655%
Barb	40,940	98	139	41,245	0.575%
平均值	40,203	99	140	40,510	0.589%

4.4.3 執行效率討論

本小節討論在建立本技術之加密執行效率。由於本技術主要是在結合密碼學技術或 RA 註冊加密技術來對 JPEG 2000 或 JPSEC 編碼串流進行加密，並將建立 PVL 與 KVL 額外資訊，因此，其執行效率的探討則著重於 PVL 與 KVL 建立過程所佔用總加密時間的比例。從 3.2 節所介紹的 PVL 與 KVL 演算法可看出，以整個編碼串流來看，各位元組均只進行語法檢測一次，其時間複雜度(Big-O)均為 O(n)。為說明本技術建立 PVL 與 KVL 額外資訊之效率，本研究使用 AES 加密演算法實際對 6 張實驗圖像進行加密，並記錄額外執行時間，如表 4.5 所示，其中所謂額外時間是指從封包語法檢測開始、經過封包切割、KVL 與 PVL 陣列的產生，將 SEC 區段嵌入至主檔頭，最後輸出加密圖像的執行時間；而總時間則從使用者輸入私密金鑰後開始計算至加密圖像輸出的執行時間。

表 4.5 加密實驗圖像額外執行時間(秒)

圖像	額外時間	總加密時間	所佔比例
Lena	0.078	78.75	0.099%
F16	0.094	79.782	0.118%
Baboon	0.109	100.016	0.109%
Boat	0.094	85.641	0.110%
Peppers	0.094	80.891	0.116%
Barb	0.109	86.328	0.126%

由表 4.5 得知，本技術所佔用的額外時間均介於 0.078~0.11 秒之間，因此並不會因為套用的加密工具不同而造成加密過程中有額外過重的負荷。

4.4.4 安全性討論

由於本加密技術主要目的在輔助標準工具及已註冊工具進行加密以達到相容性目的，因此，對密碼分析而言，加密後影像的安全性則是基於實際加密工具的演算法強度。而在現代的密碼學中，不讓惡意者知道加密演算法來保護影像檔案的方式已不符合密碼演進潮流[12]。換句話說，近代的密碼學的加密演算法大都已公布週知，其安全性則建立在金鑰長度和演算法的強度。

另一方面，本技術將超過 0xFF8F 中 0xFF 位元組換成 0xFE，對加密後的封包而言，並不會提供破密者任何資訊，反而多了另一層保護，即使是攻擊者從 KVL 陣列獲得原 0xFF 之位置，最多也只能復原加密後之密文，其安全性仍在使用之密碼學演算法。最近的研究[13]指出，如果只加密 JPEG 2000 封包，而不加密封包檔頭，則攻擊者可能會利用封包檔頭的資訊獲得影像中物件相當粗糙的輪廓，雖然如此，攻擊者從這方面可得到的原始影像資訊非常有限，若在應用上有這方面安全上的疑慮，則應避免只對封包內容加密。

5.結論

在網際網路快速發展的現在，影像安全性的需求與日俱增，JPEG 2000 影像符合高壓縮率、高品質的優點，若再配合 Motion-JPEG 2000 的技術，在未來可能成為各方面應用的主流。JPSEC 已經完成對影像安全的相關規範，本文提出的方法則是根據 JPSEC 語法規範，設計出已註冊安全工具，其具有下列優點：

(1) 使得加密後的 JPSEC 編碼串流同時符合 JPEG 2000 Part 1 及 Part 8 的規範。並沒有因為對影像進行加密，就喪失標準解碼器對加密影像的相容性。並且無論套用之加

密工具是屬於區塊或串流加密，在加密後，均可由本方法來保持加密影像的高相容性。

(2) 在符合 JPSEC 的規範之下，除了可以使用已註冊加密工具只對封包內容進行加密，也能套用規範內所訂之標準加密工具。這讓未來安全性更高的加密方法，也能透過本文所提方法對 JPEG 2000 影像進行相容性加密。

實驗結果顯示，在加密過程中所產生的額外解密資訊可以被嵌入在主檔頭中而不會造成標準解碼器解碼的錯誤。而加密後的 JPSEC 編碼串流則可被符合 JPEG 2000 Part 1 標準解碼器正確解碼，也同時可被支援 JPSEC 的解碼器正確解碼及解密，亦即本文所提出的加密技術可以符合高相容性的需求。因此，本文所提出的加密技術具有實用性及安全性。

誌謝

本研究為中華民國行政院國家科學委員會專題研究計畫部分成果，計畫編號：NSC 98-2221-E-606 -015。

參考文獻

[1] Cox, I., Miller M., and Bloom J., Digital Watermarking, Morgan Kaufmann, 2002.

[2] Information Technology - JPEG 2000 Image Coding System, ISO/IEC Final Committee Draft 15444-1, 2000.

[3] Rabbani, M. and Joshi, R., "An Overview of the JPEG 2000 Still Image Compression Standard," *Signal Processing: Image Communication*, Vol. 17, No. 1, pp. 3-48, Jan. 2002.

[4] Christopoulos, C., Skodras, A., and Ebrahimi, T., "The JPEG 2000 Still Image Coding System: An Overview," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 1103-1127, Nov. 2000.

[5] Information Technology – JPEG 2000 Image Coding System–Part8 : Secure JPEG 2000, ISO/IEC International Standard 15444-8, Apr. 2007.

[6] Wu, H. and Ma, D., "Efficient and Secure Encryption Schemes for JPEG 2000," *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Singapore, Vol. 5, pp. 869-872, May 2004.

[7] Wu, Y. and Deng, R., "Compliant Encryption of JPEG 2000 Code-streams," *Proceedings of the IEEE International Conference on Image Processing, Singapore*, Vol. 5, pp. 3439-3442, Oct. 2004.

[8] Yang, Y., Zhu, B.-B., Li, S., and Yu, N., "Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability," *EURASIP Journal on Information Security*, Vol. 2007, Article ID 56365, 13 pages, Nov. 2007.

[9] Grangetto, M., Magli, E., and Olmo, G., "Multimedia Selective Encryption by Means of Randomized Arithmetic Coding," *IEEE Transactions on Multimedia*, Vol. 8, No. 5, pp. 905-917, Oct. 2006.

[10] Liu, J.-L., "Efficient Selective Encryption for JPEG 2000 Images Using Private Initial Table," *Pattern Recognition*, Vol. 39, No. 8, pp. 1509-1517, Aug. 2006.

[11] Engel, D., Stutz, T., and Uhl, A., "Format-Compliant JPEG2000 Encryption in JPSEC: Security, Applicability, and the Impact of Compression Parameters," *EURASIP Journal on Information Security*, Vol. 2007, Article ID 94565, 13 pages, Nov. 2007.

[12] Stallings, W., Cryptography and Network Security Principles and Practices, Fourth Edition, PEARSON, 2006.

[13] Dufaux, F., Wee, S., Apostolopoulos, J., and Ebrahimi, T., "JPSEC for Secure Imaging in JPEG2000,"*SPIE Proceedings—Applications of Digital Image Processing XXVII*, Colorado, USA, pp. 319-330, Nov. 2004.

[14] Mathworks, http://www.mathworks.com/

[15] InfanView, http://www.irfanview.com/