基於數位浮水印與個人資料保護與稽核

劉凱勛*　蔡昌隆**

*文化大學機械工程系數位機電所　**中國文化大學資訊工程學系

摘要

台灣政府於 99 年 4 月 27 日通過個人資料保護法[1]，旋即於 101 年公布實施。由於各機關團體與公司企業為服務客戶，多蒐集儲存很多個人資料或電子資訊，為保護個資之安全及於授權範圍之合法運用，免於遭到洩漏或惡意散播。因此，掌握個資之儲存與流向等相關安全維護與稽核甚為重要，運用浮水印或數位浮水印之技術可有效對文件資料或電子資訊註記，以加強對個資文件之保護，經結合更能達到追蹤稽核個資文件之分享途徑與儲存現況，以強化個資之整體安全防護。

關鍵詞：個資保護法，數位浮水印，個資文件

1. 研究背景

隨著資訊與網路時代迅速的發展，過去文書呈現之資料，多改為電子形式，可使用電腦輔助處理圖片、影像等多媒體資料，並於網路世界中輕鬆分享這些資料。為保護電子資料的機敏性，免於遭受竊取、竄改或洩漏等威脅暨維護所儲存之電子資料的完整性，相關個資之文書與電子資料均應妥善予以處理[10]。

近年來因網際網路的盛行，大部分的人可以輕鬆的在網路上傳送以及下載資料，而這些資訊有可能被有心人竄改或者是破壞，因而人們在使用網路中會有風險性，如何在保護資料在傳輸過程中的安全性是非常重要的。

在影像隱藏的技術中，主要影像處理可分成頻率域和空間域兩類。頻率域技術是將原始圖檔做頻率轉換，在把要機密的圖像藏入頻率係數中，而空間域則不必做任何轉換，可直接在原始圖檔中做處理，將機密的圖像藏在掩蓋的影像中。

空間域技術中有一方法叫做(LSB)[2]，它的方法為將機密圖像藏入掩蓋影像在最不重要的位元當中，雖然使用方法簡單，但是此方法所獲得的影像品質較佳，較不易被人發現，缺點是易遭受破壞。其他諸如頻率域的資料隱藏大多存在資料隱藏量低的問題，而若當機密圖像藏入掩蓋影像的位元數量越多時，偽裝影像的品質相對越差，假如有心人想要竊取檔案很容易發現此圖檔已經藏入機密圖像。

2. 數位浮水印

個資電子資料係經資料生成前之資料搜集階段，於處理後所建立，其生命週期如下圖 1。對於個資電子資料另增加保密措施後儲存及保存，並於應用過程中採取適當保護措施及安全的網路傳輸進行資料交換，最後當電子資料不再有儲存或存在之價值時，或需要銷毀時，電子資料尚須經資料殘存的處置以確保完整之資料銷毀，相關處理流程如圖所示。

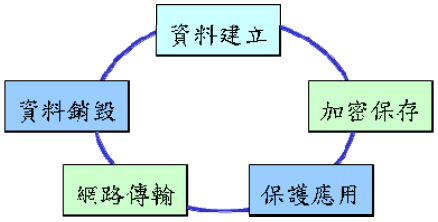

圖 1：個資電子資料之生命週期圖

2.1. 數位浮水印嵌入方法

嵌入浮水印方法可分為空間域與頻率域，無論想隱藏的資料文字、文件、影像、聲音、影音或多媒體資訊，我們都可以將相關資料轉換成我們所要的特定格式，如二位元資料序列串。而資料鑲嵌的基本計算公式可以用下列數學式子來描述：Raw_Image(原始影像)+Hidden_data(隱藏資料)=Stego_image(已鑲嵌影像) 亦可使用權重因子(如金鑰控制器)做為調整參數，以改善資料隱藏效能，其計算公式可修正如下:Raw_Image(原始影像)+weight*K(key)*H(隱藏資料)=Stego_image(已鑲嵌影像) 於空間域，較為普遍的鑲嵌技術有最不重要位元(LSB, least significant bit)、Patch work、像素異動(Pixel difference)flippable 與加法 Addition modulo、質方圖差異法(histogram difference)等方法[3][4][5][6]。在頻率域，較為廣泛應用的鑲嵌技術有數位餘弦轉換(Discrete Cosine Transform)、數位小波轉換(Discrete Wavelet Transform)、Fresnel 轉換、數位傅利葉轉換(Discrete Fourier Transform)及 Fractal 轉換等諸多方法。其他還有 Quantization index modulation(又稱為 Dither Transform)及 Radon transform 等轉換方法。亦可使用結合空間域與頻率域之混合處理機制。有關空間域與頻率域之嵌入法概略如下:

2.2 空間域(spatial domain)

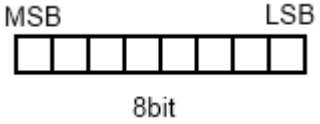

圖 2 空間域藏入位置

此方法主要是利用每個像素編碼中之 LSB(least significant bit)位元的值來藏入浮水印或擬隱藏資訊之值，如圖 2 所示。可取最右邊的 1 或多個位元以供隱藏資訊，將其內容利用 and 或 or 運算來更改其中的值，將內容更換為浮水印或擬隱藏資訊。

此方法之優點為能藏入較多資訊且透明性較高，程式執行速度又快，唯其缺點是強健性不足，使用一些簡單的方法就可將浮水印破壞掉，此方法屬於早期的數位浮水印技術。

2.3 頻率域 (frequency domain)

近年來的浮水印技術大多使用此類，頻率域的處理又可分為以下幾種：(1)離散餘弦轉換(Discrete Cosine Transform)：主要有 2 種做法，其中一種將影像切割成如 8*8 之區塊並採用量化對照表如下表 1 進行處理，另一種為亦將影像切割成類如 8*8 或 16*16 等 2N*2N 之區塊，以 DCT 函式進行計算其 AC 與 DC 值，再執行 IDCT 回復成影像[7]。

表 1：8*8 DCT 轉換對照表

6	1	0	6	4	0	1	1
2	2	4	9	6	8	0	1
4	3	6	4	0	7	9	6
4	7	2	9	1	7	0	2
8	2	7	6	8	09	03	7
4	5	5	4	1	04	13	2
9	4	8	7	03	21	20	01
2	2	8	8	12	00	03	9

(2) 離散小波轉換 (Discrete Wavelet Transform)，如圖 3 執行 DWT 轉換，將影像拆解成 3 階 10 個次波段處理，再執行 IWT 回復成影像[8]，此法之資訊隱藏量不大。

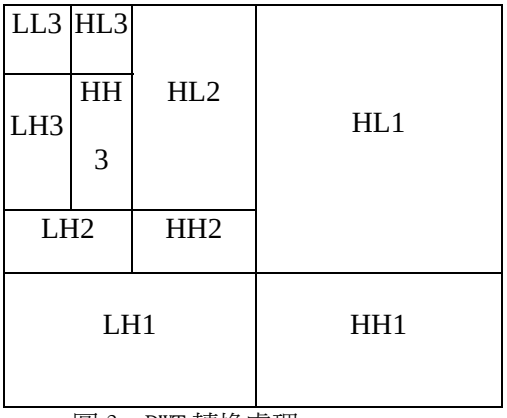

圖 3：DWT 轉換處理

(1) 離散傅利葉轉換 (Discrete Fourier Transform)：此法需計算 FFT，取其 Amplitude(絕對值)並做 Normalization，再執行 IDFT 回復成影像[9]。

頻率域處理方法的作法是先將原圖轉換到頻率域[3]，經於頻率域藏入浮水印或擬隱藏資訊至頻率係數中後，再執行 inverse 反處理將頻率域之資料

轉換回空間域之影像資料。此類方法之優點為具有較高之強健性，不容易被破壞，但可藏入的資訊相對於空間域則大幅減少。

3. 實驗結果

為有效追蹤個人資料之處理與流向，本論文中，擬藏入個資影像中之資料包含原始收集此個資之單位(使用符記或代碼註記)、後續分發之相關處理單位(使用符記或代碼註記)，並加入時間戳記以利追蹤。

本論文之實驗處理採用離散小波轉換資訊隱藏處理機制如圖 4 所示:

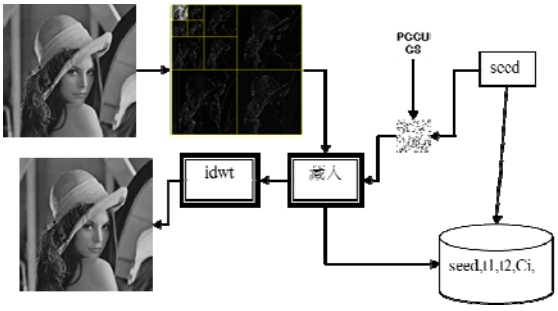

圖 4：離散小波轉換資訊隱藏處理機制

其詳細之處理步驟概略如下：

Step 1:讀取一張影像和浮水印 w，將影像以 DWT 轉換至頻率域。

Step 2:浮水印數值改為 0 和 1 之後，先使用(LFSR)的方法取出一個亂數種子產生亂數，設影像大小為 m，產生出 n 個數在做(n div m),(n mod m)即為打散後座標。

Step 3:選取 2 個 threshold T1 與 T2 與 ，使得 T2 > T1 > 。

Step 4:選擇 LH3,HL3,HH3 這 3 個頻帶來當做藏入的位置。

Step 5:將 LH3、HL3、HH3 等所有係數依序掃描一次，取 Ci (i=1..n)拿來做嵌入 wi (i=1..n)的位置，當滿足 T2 > | Ci | >T1。

Step 6:將選中的位置以 T 取代，並且記錄其位置：

If Ci >0: wi = 1 Þ Ci = T2

wi = 0 Þ Ci = T1

If Ci <0: wi = 1 Þ Ci = -T2

wi = 0 Þ Ci = -T1

Step 7:儲存已修改的係數位置 C1C2C3…Cn、T1 、T2、 與產生亂數的種子， 以備之後萃取出浮水印時使用。

Step 8:執行 Inverse DWT 將頻率域之資訊處理轉回空間域影像。

如此即完成資料之鑲嵌作業。

4. 結論

運用數位浮水印的方法可以讓文件變得更加安全，也可以防止有人惡意破壞文件；可有效追蹤及稽核文件之現況，以達個資保護。本論文針對個資文書與電子檔案之保護、作業處理程序、完整性驗證以及流向稽核等方面，經分析探討後所提出之較佳實現機制，可提供企業、機關團體乃至個人對個資電子資訊之安全維護應用。

參考文獻

[1] 法務部，個人資料保護法，網址：http://www.moj.gov.tw/lp.asp?ctNode=28007&CtUnit=805&BaseDSD=7&mp=001，上網日期：2013 年 10 月 20 日

[2] A. D. Ker, “Improved detection of LSB steganography in grayscale images,”In Proc. Information Hiding Workshop, Vol. 3200, Springer LNCS, pp.97-115, 2004.

[3] D. Yu, F. Sattar, and B. Barkat, “Multiresolution Fragile WatermarkingUsing Complex Chirp Signals for Content Authentication,” PatternRecognition, May 2006, Vol. 39, Issue 5, pp. 935-952.

[4] G. Caronni, “Assuming Ownership Rights for Digital Images”, Proceedings Reliable IT System, VIS 1995, 1995

[5] S. H. Liu, H. X. Yao, W. Gao, and Y. L. Liu, “An Image Fragile WatermarkScheme Based on Chaotic Image Pattern and Pixels-pairs,” AppliedMathematics and Computation, Fed. 2007, Vol.185, Issue 2, pp. 869-882.

[6] S. Suthaharan, “Fragile Image Watermarking Using a Gradient Image forImproved Localizatioin and Security,” Pattern Recognition Letters, Dec.2004, Vol.25, Issue 16, pp. 1893-1903.

[7] Y. K. Lai, and Yu. F.Lai, “A reconfigurable IDCT architecture for universal video decoders”, IEEE Trans. Consumer Electronics: Express Briefs, vol. 56, no. 3, pp. 1872 -1879, Aug. 2010.