投影式高品質彩色影像之可變動資料嵌入研究

Fidelity Colour Multimedia Image with Adaptive Data Hiding on Projection Dimensions

江文雅　王旭正　林曾祥
中央警察大學資訊管理系所
sjwang@mail.cpu.edu.tw

摘要

資訊隱藏技術逐年發展，在空間域及頻率域方面均陸續有新技術的提出。本篇文章主要針對彩色影像空間域的藏密技術進一步強化逼真度並維持高藏密量。首先我們以彩色影像單一像素為基本單位，並將像素位元組作投影動作，透過投影平面的切割、編碼，投影像素位置的轉換，來完成藏入機密訊息的動作。我們所提出的藏密方法完全不會擴張 cover image 原來的大小，且在萃取機密訊息時亦不需要原圖的存在。在藏密量方面不僅達成了藏密技術研究的高容量要求，對於嵌入訊息後的影像品質也達到了相當的水準。藉此，我們的研究有效地在藏入高容量的彩色媒體圖裡，提供了更好的藏密品質。

Abstract

The technique of information hiding is booming in recent decades. There have been considerably explored in the spatial domain and frequency domain for information hiding researches. In this paper, we propose a projection-based data hiding scheme in spatial domain for colour images, where the image quality is remarkably enhanced as well as the higher capacity is still guaranteed In our scheme, we firstly take one pixel in the cover image as the basis, and project it onto a plane. Then, the algorithm of embedding process is proposed in terms of the segment, coding and transformation of location to fulfill the data hiding in the colour image systems. In our paper, not only the size of the cover image remains the same, but also the cover image is no long required in the course of extracting the embedding information. As a result, our paper is to offer an efficient scheme that both achieves the great fidelity and high capacity for the colour multimedia image systems.

關鍵詞：資訊隱藏(information hiding)、藏密量(capacity)、高品質(high quality)、像素投影(pixel projection)、平面切割(plane division)

一、 Introduction

資訊隱藏(Information Hiding)或藏密學(Steganography)是一門將機密訊息藏入任何載體的學問。其緣起可追溯至古希臘時代，隨著時代的進步與科技的發展，現今的資訊隱藏技術研究多植基於網際網路及數位載體上，依據其存在目的不同，而有不同的發展重點。每年均有許多更為精進的資訊隱藏技術被發展出來，不論在藏密量或者是圖像品質方面，都有相當大的進步。資訊隱藏的領域涵括空間域、頻率域等兩大技術。其研究範圍則因藏密的目的而有不同，例如：在藏密技術的研究中，以藏密量、藏密品質為要求標的；在浮水印研究中，則強調其不可察覺性及強韌性的達到。

在早期的研究裡，有部份重要的基礎研究文章，諸如 Bender et al.[1] 整理有關資訊隱藏的技術研究。Marvel et al.[2] 探

討有關將機密訊息藏入影像載體的研究。近年來，更有許多資訊隱藏研究技術的提出。2003 年 Thien and Lin[3] 提出以模函數為基礎的高容量訊息隱藏技術，將訊息藏於影像中。2005 年 Wang [5] 提出改良式的模運算，將機密藏入影像中，且達到萃取機密不需使用輔助對照表的目標。2007 年 Tsai and Wang [4] 提出以 3D 空間為假想的藏密方法，將機密訊息藏入彩色影像中，不僅達到品質與容量的要求，且能抵抗部份的藏密攻擊。2007 年 Wang and Tsai [6] 利用 best-block matching 與 k-means clustering 概念，同樣發展出高容量與高品質的藏密技術。綜觀過去所提出之資訊隱藏研究文獻，不論是在彩色影像或灰階影像的研究領域，大都著墨於藏密量與藏密品質的提昇，然卻甚少考慮到載體藏密空間的可變動性。本文所提出的方法除加強藏密量與影像品質外，更同時附加了藏密空間的變動技術。同一張載體影像可考量影像大小、藏密量多寡而選用可變動性的藏密方法，使得資訊隱藏的過程更加的有彈性與選擇性。我們所提出的藏密技術，主要為抽取彩色影像單一像素作平面投影，透過投影平面的切割編碼與投影像素位置的改變，來完成藏入機密訊息的動作，且在萃取機密訊息的過程中，不需使用原圖，僅需掌握關鍵資訊即可進行解密動作。

本研究論文結構說明如下: 第二節中首先提到資訊隱藏領域的基礎知識。第三節提出我們的藏密演算法，包含子平面的切割方式 type-I 與 type-II 的介紹。第四節是實例說明與實驗結果的展示。第五節為分析與討論。並在第六節中作結論。

二、 Preliminaries

(一) 空間域與頻率域

資訊隱藏的研究領域相當廣泛，主要可區分為空間域(spatial domain)與頻率域(frequency domain)等兩大技術。近年來更有視覺密碼技術的研究與發展。空間域的藏密技術是以置換像素位元為基礎，大多是取代圖像像素中較不重要的位元，以降低因嵌入訊息導致的圖像改變。LSB (least significant bit)的藏密方法是最典型的例子。假設一灰階圖像像素值為(00101101) ，機密位元為 10。為了降低機密位元嵌入後對原始圖像的改變，因此，我們挑選最右邊的二個位元作置換，則嵌入機密位元後的圖像像素值為(00101110)。這種直接置換像素位元的資訊嵌入方法稱為空間域的嵌入技術。

頻率域的藏密技術是將圖像經過轉換處理後，再針對人類感知較不敏感的頻率區塊作機密訊息的藏入。圖像經過轉換後可區分為高頻帶以及低頻帶，由於人類肉眼對於高頻帶區域的辨識較不敏感，其內容的細微改變並不容易遭察覺。因此在頻率域的藏密技術便是將機密訊息藏入高頻處。目前常見的頻率域技術則有離散餘弦轉換(DCT)與離散小波轉換(DWT)。

(二) 彩色影像 PSNR 值的計算

影像在藏入機密訊息的過程中，部份像素內容會遭到修改，使得原始圖像與嵌入訊息後的影像有部份的改變。在資訊隱藏領域的研究中，陸續提出的嵌入技術除要求高的藏密量以外，影像品質也是要求的重點之一。若是能將影像嵌入訊息前後的改變降至最低，則稱該技術可達到極佳的嵌入品質。而衡量影像嵌入訊息前後改變的指標就是 PSNR 值的計算，其單位為 dB。在灰階影像中 PSNR 值的定義如下：

$$PSNR = 10 \times \log_{10}(\frac{255^2}{MSE}) \quad MSE = \frac{1}{wh}\sum_{i=1}^{w}\sum_{j=1}^{h}(x_{ij} - y_{ij})^2 \tag{1}$$

MSE 指的是 mean square error，其中 w 與 h 分別為影像的像素尺寸寬跟高，x_{ij} 是 cover image 的第 ij 個像素值；y_{ij} 則是 stego image 的第 ij 個像素值。

在彩色影像中，PSNR 值定義如下：

$$PSNR = 10 \times \log_{10}(\frac{255^2}{MSE_{avg}}) \quad MSE = \frac{1}{wh}\sum_{i=1}^{w}\sum_{j=1}^{h}(x_{ij} - y_{ij})^2 \tag{2}$$

其中 MSE_{avg} 指的是彩色影像 RGB 個別的計算 MSE 後的平均值。

三、 Our scheme

在我們所提出的方法中，首先將機密訊息或影像轉換成連續的二進制位元表示，稱之為 bi-secret。並假設一次取 bi-secret 中的 *a*-bit 藏入 cover image 的一個像素。Cover image 為一彩色影像，由左至右，由上至下，一次取出一個像素，並將一個像素的 RGB 分離出來用二進制方式表示，$(R_{7...}R_1R_0,G_{7...}G_1G_0,B_{7...}B_1B_0)$ 。假設在一次的藏入動作中，各取 RGB 的最後 *b*-bit 作為藏入 secret 的位置，稱為挑選像素 s-pixel (select pixel)。

在我們方法中，我們並非將 bi-secret 直接藏入 cover image 的 s-pixel，而是將每一個 s-pixel 的 *b*-bit 數值想像為空間中的一個點 $(R_{b...}R_1R_0,G_{b...}G_1G_0,B_{b...}B_1B_0)=(X,Y,Z)$，並先作一投影的動作。我們以每一個像素的第 $R_{b+1}G_{b+1}$ 作為投影的判斷依據，若為 00 則投影至 x-y-plane 平面；01 投影至 y-z-plane 平面；10,11 則投影至 x-z-plane 平面。將 s-pixel 作投影後，接著是將投影平面分割成多個子平面並編號。子平面的切割有兩種形式分別為 type-I 與 type-II。在 type-I 中，機密位元等同子平面的編號；在 type-II 中，機密位元為子平面編號的末 *a*-bit。

(一) 投影平面的分割

在同一個機密影像中，任何投影平面均適用同一種分割方式，投影平面的分割與其從 cover image 中取出的 s-pixel 有關。假設一次取 cover image 像素中，各 RGB 位元組的最右邊 *b*-bit 作為藏入 secret 的位置，則投影平面將被分割為 2^{2b} 個子平面，擇定子平面編號起始位置 P_{start} 後，其它子平面編號順序則依 P_{start} 上、下、左、右編號，每一子平面包含左下角座標點。另外，P_{start} 的值表示子平面編號起點，投影平面自左而右，自下而上，以 $0\sim2^{2b}-1$ 分別代表 P_{start} 的值。舉例來說：假設一次取一個像素 RGB 的最後 1 個 bit 作為藏入 secret 的位置，則投影平面分割成 $2^2=4$ 個子平面，擇定左上方之子平面為編號起點($P_{start}=2$)後，依編號方式上、下、左、右編號，已編號或無分割子平面處則略過，編號方式如圖 1 所示。

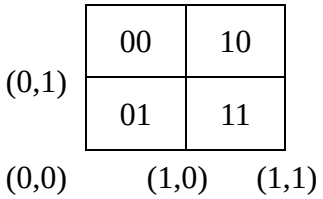


圖 1 投影平面的分割

若 b 等於 2，則投影平面分割成 $2^4=16$ 個子平面，擇定左下角子平面為編號起點($P_{start}=0$)，依編號方式上、下、左、右編號，已編號或無分割子平面處則略過，編號方式如圖 2 所示。

(0,4)	0110	1010	1101	1111
(0,3)	0011	0111	1011	1110
(0,2)	0001	0100	1000	1100
(0,1)	0000	0010	0101	1001
(0,0)	(1,0)	(2,0)	(3,0)	(4,0)

圖 2 投影平面的 2^4=16 子平面分割

(二) type-I

在 type-I 中，機密位元等同子平面的編號。我們將 cover image 的一個像素分別取 RGB 的 *b*-bit 來藏入 a 個機密位元。a 與 b 的關係為(a=2b)。首先，確定投影平面後，將投影平面切割成為(2^bx2^b)個子平面並以 *2b*-bit 作編號。接著將所取的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)轉換成十進制的(X_1,Y_1,Z_1)值，依據投影平面取出其中的(X_1,Y_1), (Y_1,Z_1)或(X_1,Z_1)值稱為平面上的投影點，找出投影點所在的子平面編號。接著，一次取出 a 個機密位元，並在投影平面上找到與機密位元相同的子平面編號，然後將 s-pixel 的投影點移至該子平面的相對位置。將新的投影點(X',Y'),(Y',Z')或(X',Z')轉成二進制($R'_{b...}R'_1R'_0$,$G'_{b...}G'_1G'_0$,$B'_{b...}B'_1B'_0$)取代原來的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)，則完成以一個像素中的 *b*-bit 來藏入 a 個機密位元的動作。為有效完成高品質的彩色媒體圖像的資訊嵌入，我們提出 type-I 與 type-II 等各兩個 ***embedding process***， ***extracting process algorithms***，細部說明如下:

Algorithm 1: (embedding process)

輸入：彩色影像(cover image)，機密影像，數值 a 與 b，子平面編號起始位置 P_{start}。

輸出：stego image。

step1：一次抽取 cover image 中的一個像素，其 RGB 二進制表示方式為($R_{8...}R_1R_0$,$G_{8...}G_1G_0$,$B_{8...}B_1B_0$)=(X,Y,Z)。

step2：以第 $R_{b+1}G_{b+1}$ 作為投影的判斷依據，若為 00 則投影至 x-y-plane；01 投影至 y-z-plane；10,11 則投影至 x-z-plane。

step3：分割投影平面成為(2^bx2^b)個子平面並以 *2b*-bit 作編號。(a=2b)

step4：將所取的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)轉換成十進制的(X_1,Y_1,Z_1)，並依 step2 所決定的投影平面，取出(X_1, Y_1),(Y_1,Z_1)或(X_1,Z_1)值，找出投影座標點所在的子平面編號。

step5：一次取 a 個機密位元，並在投影平面上找出等同機密位元的子平面編號，其所含座標點為(X',Y'),(Y',Z')或(X',Z')。

step6：將(X',Y'),(Y',Z')或(X',Z')轉成二進制($R'_{b...}R'_1R'_0$,$G'_{b...}G'_1G'_0$), ($G'_{b...}G'_1G'_0$,$B'_{b...}B'_1B'_0$), ($R'_{b...}R'_1R'_0$,$B'_{b...}B'_1B'_0$)取代原來的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$),($G_{b...}G_1G_0$,$B_{b...}B_1B_0$), ($R_{b...}R_1R_0$,$B_{b...}B_1B_0$)。

step7：重覆 step1~6 完成嵌入機密位元動作。

Algorithm 2: (extracting process)

輸入：stego image，數值 a 與 b，子平面編號起始位置 P_{start}。

輸出：機密影像。

step1：一次抽取 stego image 中的一個像素。

step2：依資訊 a,b 與子平面編號起始值 P_{start}，解出投影平面分割編號樣式。

step3：以所取像素第 $R_{b+1}G_{b+1}$ 作為投影的判斷依據，若為 00 則投影至 x-y-plane 平面；01 投影至 y-z-plane 平面；10,11 則投影至 x-z-plane 平面。

step4：將所取投影像素的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)轉換成十進制的(X_1,Y_1,Z_1)，並辨識其在投影平面上子平面

的編號即為機密位元。

step5：重覆 step1~4 完成萃取機密位元動作。

(三) type-II

在 type-II 中，機密位元等同子平面編號的末 a 個位元。我們將 cover image 的一個像素分別取 RGB 的 *b*-bit 來藏入 a 個機密位元。其中 a 與 b 的關係為(a<2b) 。首先，確定投影平面後，將投影平面切割成為(2^bx2^b)個子平面並以 *2b*-bit 作編號。接著將所取的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)轉換成十進制的(X_2,Y_2,Z_2)值，依據投影平面取出其中的(X_2,Y_2),(Y_2,Z_2)或(X_2,Z_2)值稱為平面上的投影點，找出投影點所在的子平面編號(P_n)。一次取出 a 個機密位元，並在投影平面上找到末 a 個位元與機密位元相同的子平面編號，計有 $2^{(2b-a)}$ 個子平面符合條件，稱為 P_t t=0,1…$2^{(2b-a)}$，接著計算 P_n 與 P_t 間的水平距離平方和與垂直距離平方和(SHV_t)，以 SHV_t 最小者為機密位元所在的子平面，並將投影點移至該子平面所包含的投影點，將新的投影點(X',Y'),(Y',Z')或(X',Z')轉成二進制($R'_{b...}R'_1R'_0$,$G'_{b...}G'_1G'_0$), ($G'_{b...}G'_1G'_0$,$B'_{b...}B'_1B'_0$)或($R'_{b...}R'_1R'_0$,$B'_{b...}B'_1B'_0$)取代原來的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$),($G_{b...}G_1G_0$,$B_{b...}B_1B_0$)或($R_{b...}R_1R_0$,$B_{b...}B_1B_0$)，則完成以一個像素中的 *b*-bit 來藏入 a 個機密位元的動作。

在本文的方法中，藏密者僅需將 stego image 以及 a,b,子平面編號起始位置 P_{start} 等資訊傳送予解密者，則接收者可在不需原圖的情況下，直接將藏在 stego image 中的機密位元解出來。

Algorithm 3: (embedding process)

輸入：彩色影像(cover image)，機密影像，數值 a 與 b，子平面編號起始位置 P_{start}。

輸出：stego image。

step1：一次抽取 cover image 中的一個像素，其 RGB 二進制表示方式為($R_{8...}R_1R_0$,$G_{8...}G_1G_0$,$B_{8...}B_1B_0$)=(X,Y,Z)。

step2：以第 $R_{b+1}G_{b+1}$ 作為投影的判斷依據，若為 00 則投影至 x-y-plane 平面；01 投影至 y-z-plane 平面；10,11 則投影至 x-z-plane 平面。

step3：分割投影平面成為(2^bx2^b)個子平面並以 *2b*-bit 作編號。(a<2b)

step4：將所取的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)轉換成十進制的(X_2,Y_2,Z_2)，並依 step2 所決定的投影平面，取出(X_2,Y_2),(Y_2,Z_2)或(X_2,Z_2)值，找出投影座標點所在的子平面編號 P_n。

step5：一次取 a 個機密位元，並在投影平面上找出末 a 個位元等同機密位元且距離投影座標點最近的子平面編號，其所含座標點為(X',Y'),(Y',Z')或(X',Z')。

step6：將(X',Y'),(Y',Z')或(X',Z')轉成二進制($R'_{b...}R'_1R'_0$,$G'_{b...}G'_1G'_0$), ($G'_{b...}G'_1G'_0$,$B'_{b...}B'_1B'_0$)或($R'_{b...}R'_1R'_0$,$B'_{b...}B'_1B'_0$)取代原來的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$),($G_{b...}G_1G_0$,$B_{b...}B_1B_0$)或($R_{b...}R_1R_0$,$B_{b...}B_1B_0$)。

step7：重覆 step1~6 完成嵌入機密位元動作。

Algorithm 4: (extracting process)

輸入：stego image，數值 a 與 b，子平面編號起始位置 P_{start}。

輸出：機密影像。

step1：一次抽取 stego image 中的一個像素。

step2：依資訊 a,b 與子平面編號起始值 P_{start}，解出投影平面分割編號樣式。

step3：以所取像素第 $R_{b+1}G_{b+1}$ 作為投影的判斷依據，若為 00 則投影至 x-y-pl

ane 平面;01 投影至 y-z-plane 平面;10,11 則投影至 x-z-plane 平面。

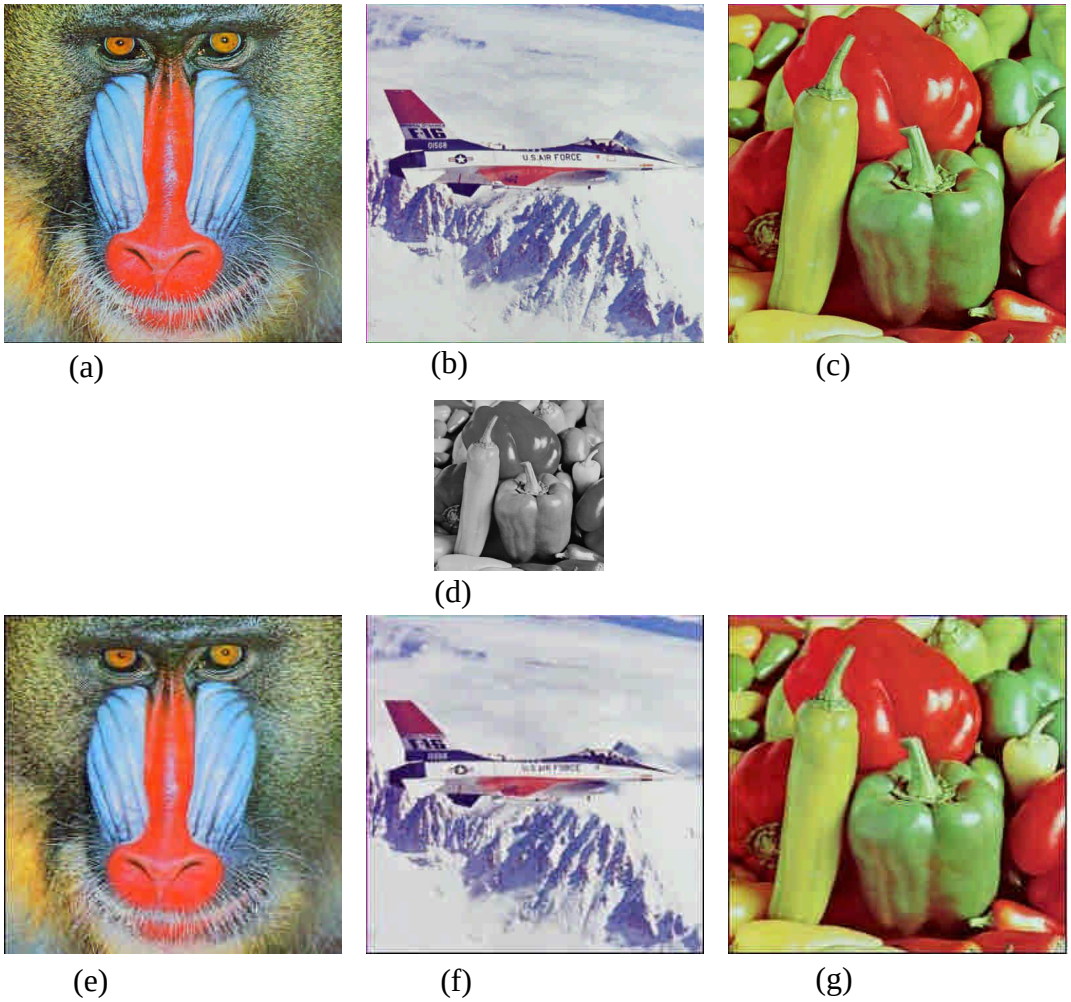
step4：將所取投影像素的($R_{b...}R_1R_0$,$G_{b...}G_1G_0$,$B_{b...}B_1B_0$)轉換成十進制的(X_2,Y_2,Z_2)，並辨識其在投影平面上子平面編號的末 a 個位元即為機密位元。

step5：重覆 step1~4 完成萃取機密位元動作。

四、 Empirical Experiments

(一) type-I

此例中，我們分別以灰階影像與隨機位元作為嵌入的機密訊息，實作 type-I 結果。首先設定 a=2, b=1(機密位元為 2-bit，且一次取一個像素中的任二組 RGB 的最後 1 個 bit 作為嵌入機密位元的位置)。圖 3 顯示以灰階影像作為機密訊息的實驗結果，圖 3(a),(b),(c)為彩色影像 Baboon,F16, Pepper 作為 cover image(512x512 像素)，圖 3 (d)為機密灰階影像 Pepper (256 x 256 像素)，藏入機密訊息後的 stego image 如圖 3 (e),(f),(g)所示。圖 4 顯示以隨機位元作為機密訊息的實驗結果。圖 4(a),(b),(c)為彩色影像 Baboon,F16,Pepper 作為 cover image(512x512 像素)，藏入隨機機密訊息後的 stego image 如圖 4(d),(e),(f)所示。另實驗數據 PSNR 結果如表一所示。



(a) (b) (c)

(d)

(e) (f) (g)

圖 3 typeI 彩色影像嵌入灰階影像實驗結果

(a) cover image“Baboon” (b) cover image “F16” (c) cover image“Pepper”

(d) secret image “Papper”

(e) stego image“Baboon” (f) stego image “F16”(g) stego image“Pepper”

(a) (b) (c)

(d) (e) (f)

圖 4 typeI 彩色影像嵌入隨機訊息實驗結果

(a)cover image“Baboon”(b)cover image “F16”(c)cover image“Pepper”

(d)stego image“Baboon”(e)stego image “F16”(f)stego image“Pepper”

表一

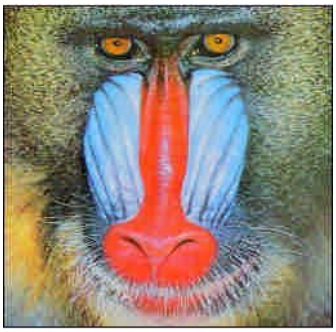
type-I				
secret	gray-level image (256x256x8 bits)		random generated (512x512x2 bits)	
cover image	P_{start}	**PSNR**	P_{start}	**PSNR**
Baboon	3	**52.913**	1	**52.941**
F16	1	**52.909**	0	**52.957**
Peppers	1	**52.914**	0	**53.061**

(二) type-II

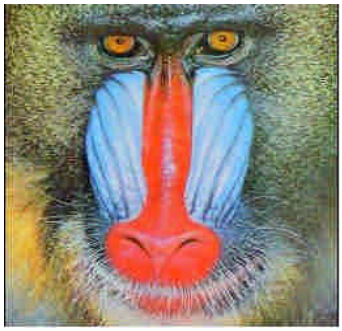
此例中，我們分別以灰階影像與隨機位元作為嵌入機密訊息，實作 type-II 結果。首先設定 a=3,b=2,3,4(機密位元為 3-bit，且一次取一個像素中的任二組 RGB 的最後 2,3 或 4 個 bit 作為嵌入機密位元的位置)。圖 5 顯示以灰階影像作為機密訊息的實驗結果。圖 5(a)為彩色影像 Baboon 作為 cover image (512 x512 像素)。圖 5 (b)為機密灰階影像 Pepper (256 x 384 像素)，藏入機密訊息後的 stego image 如圖 5(c),(d),(e)，其中 b 值分別設定為 2,3,4。圖 6 顯示以隨機位元作為機密訊息的實驗結果。圖 6 (a)為彩色影像 Pepper 作為 cover image(512x512 像素)，藏入隨機機密訊息後的 stego image 如圖 6 (b),(c),(d) 所示，其中 b 值分別設定為 2,3,4。另實驗數據 PSNR 結果如表二及表三所示。

(a)

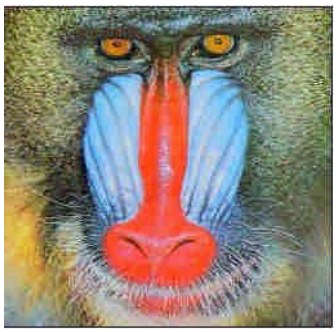
(b)



(c) b=2



(d) b=3



(e) b=4

圖 5 typeII 彩色影像嵌入灰階影像實驗結果

(a)cover image “Baboon”(b)secret image “Pepper”

(c)stego image b=2 (d) stego image b=3 (e) stego image b=4

表二

type-II secret : gray-level image (256x384x8 bits)

cover image	b=2		b=3		b=4	
	P_{start}	**PSNR**	P_{start}	**PSNR**	P_{start}	**PSNR**
Baboon	0	**49.201**	28	**42.429**	135	**38.425**
F16	15	**48.660**	27	**42.651**	50	**38.190**
Peppers	0	**49.140**	35	**42.825**	240	**38.814**

(a)

(b) b=2

(c) b=3

(d) b=4

圖 6 typeII 彩色影像嵌入隨機訊息實驗結果

(a)cover image “Pepper”

(b)stego image b=2 (c) stego image b=3 (d) stego image b=4

表三

type-II secret : random generated (512x512x3 bits)

cover image	b=2		b=3		b=4	
	P_{start}	**PSNR**	P_{start}	**PSNR**	P_{start}	**PSNR**
Baboon	0	**49.049**	27	**42.826**	209	**38.952**
F16	0	**49.037**	21	**41.256**	78	**39.720**
Peppers	0	**49.167**	28	**42.498**	94	**39.361**

五、 Analyses and Discussions

本文所提出的資訊隱藏方法適用於 RGB 的彩色影像上。藏入步驟為一次抽取彩色影像的單一像素，並依像素 RGB 的二進制狀態擇定欲藏入的位置，透過機密位元的 bit 數與藏入位置的 bit 數的選擇並搭配不同的分割投影平面。我們可變化出多機密訊息藏入的方法，只要是可轉換為二進制表示法的資料均可成為本法的機密訊息，且藏入機密訊息後的 stego image 都具有良好的 PSNR 值。表四為本法載體大小與藏密量的關係表，藉此可顯示我們所提

的藏密技術具有相當的可變動性。藏密者可依據影像大小、機密位元量選擇不同的藏密方法，以求達到最佳的藏密品質。

本文所提出的藏密技術除了提昇藏密量與藏密品質外，另外更增加了藏密方式的變動與選擇性。表五為本法與 Tsai-Wang-scheme [4]的比較表，我們的方法不僅提供兩種藏密的技術(type-I 與 type-II)，且在 type-I 與 type-II 中，更可依據參數(a,b,P_{start})設定的不同，而有不同的藏密效果。表五中顯示我們所提出的藏密方法不僅變動性較 Tsai-Wang-scheme 高，且在相同的實驗條件下(cover image 512x512 像素；隨機產生機密訊息 512x512x3 bits)，PSNR 值皆絕對大於 Tsai-Wang-scheme [4]。

表四 藏密量表

圖像 / 方法	cover image size x*y (pixel)	單一像素取出位元數 *b*-bit	單一像素嵌入位元數 *a*-bit	機密資料量 x*y*a /8 (bytes)
type-I	512*512	1	2	2^{16}
	512*512	2	4	2^{17}
	512*512	3	6	$3*2^{16}$
	512*512	4	8	2^{18}
	512*512	5	10	$5*2^{16}$
	512*512	6	12	$3*2^{17}$
	512*512	7	14	$7*2^{16}$
type-II	512*512	1	1	2^{15}
	512*512	2	1,2,3	2^{15}~$3*2^{15}$
	512*512	3	1,2,3,4,5	2^{15}~$5*2^{15}$
	512*512	4	1,2,3…7	2^{15}~$7*2^{15}$
	512*512	5	1,2,3…9	2^{15}~$9*2^{15}$
	512*512	6	1,2,3…11	2^{15}~$11*2^{15}$
	512*512	7	1,2,3…13	2^{15}~$13*2^{15}$

表五 本文方法與 Tsai-Wang-scheme [4]在 PSNR 值的比較 (隨機機密訊息)

	Tsai-Wang-scheme [4]		**Our scheme**	
cover image	V_{max}	PSNR	b	**PSNR**
Baboon		44.134		**49.049**
F16	1/64	44.114	2	**49.037**
Pepper		44.058		**49.167**
Baboon		37.904		**42.826**
F16	1/32	37.905	3	**41.256**
Pepper		37.799		**42.498**
Baboon		31.831		**38.952**
F16	1/16	31.824	4	**39.720**
Pepper		31.722		**39.361**

六、 Conclusions

資訊隱藏技術逐年發展，在空間域及頻率域方面均陸續有新技術的提出。本篇文章主要針對彩色影像空間域的藏密技術進一步強化逼真度並維持高藏密量。我們所提出的方法首先將 cover image 的單一像素作位元抽取並投影，透過投影平面座標的位移來記錄複雜的機密訊息。有別於以往 LSB 單一機密位元置換單一最不重要位元的方法，本文所提出的方法在單一像素中可嵌入 2 至 14 個位元，藏密量的彈性顯然已大大地提高；另可選擇不同的參數設定，提昇藏密方法的可變動性。在藏密品質方面，由實驗結果中證實我們所發展的技術有著非常好的 PSNR 值與並優於過去的相關研究。藉此，我們的研究有效地在藏入高容量的彩色媒體圖裡，提供了更好的藏密品質。

參考文獻

[1] W. Bender, D. Gruhl, and N. Morimoto, “Techniques for data hiding,” IBM Systems J. 35, pp. 313-336, 1996.

[2] L.M. Marvel, C.G. Boncenet, and C.T.Retter, “Spread spectrum image steganography,” IEEE Trans. Image Process. 8, pp.1075-1083, 1999.

[3] C.C. Thien and J.C. Lin, “A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function,” Pattern Recognition 36, pp.2875-2881, 2003.

[4] Y.Y. Tsai and C.M. Wang, “A novel data hiding scheme for color images using a BSP tree,” Journal of Systems and Software, vol.80, pp.429-437, 2007.

[5] S.J. Wang, “Steganography of capacity required using modulo operator for embedding secret image,” Applied Mathematics and Computation, vol.164, pp.99-116, 2005.

[6] R.Z. Wang and Y.D. Tsai, “An image-hiding method with high hiding capacity based on best-block matching and *k*-means clustering,” Pattern Recognition, vol. 40, pp.398-409, 2007.