針對植基於像素值差異且能抵禦直方圖藏密分析之藏密法的修正

楊士鋒

環球科技大學資訊管理系

摘 要

本文指出存在於由 Zhang and Wang (2004)所提出之藏密法中之瑕疵，並提出方法加以修正。Zhang and Wang 之方法，可消除由廣為人知之像素值差異(pixel-value differencing, PVD)技術所產生之偽裝影像(stego-image)，其像素差值直方圖(pixel difference histogram)中不尋常之階梯狀圖形，故而能抵抗使用直方圖藏密分析(steganalysis)所進行之攻擊。然而，這個與用來將像素差值進行分類之範圍(range)設定有關之瑕疵，由於其不當之寬度設定，在特定情況下，會導致資料嵌入程序(data embedding process)失效。本文提出了能產生恰當之範圍寬度，以確保資料嵌入程序能成功運作之方法，用來修正此一瑕疵。

關鍵詞：資訊隱藏、藏密學、像素值差異法、PVD、直方圖藏密分析

An Amendment to the Pixel-value Differencing Based Steganographic Method Immune to Histogram Steganalysis

Shih-Feng Yang

TransWorld University. Department of Information Management

Abstract

This paper indicates a flaw in the steganographic method proposed by Zhang & Wang (2004) and proposes a method to repair it. Zhang & Wang's method can eliminate the undesired abnormal steps in the pixel difference histograms of the stego-images generated by the well-known pixel-value-differencing (PVD) technique and thus is immune to histogram steganalysis. However, under certain conditions, the flaw, which is associated with the inappropriate setting of the widths of the ranges for classifying pixel differences, can lead to the failure of data embedding process. To repair the flaw, a method for generating appropriate range widths to guarantee the success of data embedding process is proposed.

Key words： information hiding, steganography, pixel-value differencing, PVD, histogram steganalysis

壹、前言

近年來，隨著網際網路的快速發展，許多重要之資訊皆透過網際網路進行傳送。然而，由於網際網路為一公開之系統，因此，要如何確保資訊在傳送過程中不被有心人士竊取，便成了資訊安全領域中，重要的一項議題。

要確保資訊在傳送過程中不被有心人士竊取，可在傳送前，先利用如 DES (data encryption standard)或 RSA 等眾所周知之加密法進行加密。然而，加密後之訊息卻容易引起有心竊密者之注意，而嘗試進行破解。另一種確保資訊在傳送過程中不被竊取之方法，為資訊隱藏(information hiding)技術中之藏密學(steganography)技術。「steganography」一詞源於希臘文，意指「隱藏之文件(covered writing)」。與加密法不同，藏密學技術藉由將機密訊息藏入掩護媒體(cover media)中不被發現，以達到安全傳送之目的，其使用已有相當長之歷史。例如，古希臘人將信使之頭髮剃光，並將機密訊息紋於其頭皮上，待信使之頭髮長回後，再派遣至機密訊息之接收方，而接收方在將信使之頭髮剃光之後，即可取得機密訊息。又例如二次大戰時所使用之隱形墨水(invisible ink)、微點(microdot)等，均為藏密學相關之技術。而現今，由於資訊科技之發展，藏密學技術主要是利用合適之演算法，將機密訊息嵌入如影像、聲音、影片、文字等數位媒體中，以得到偽裝媒體(stego-media)，並盡力使偽裝媒體與掩護媒體間之差異達到最小。當接收方收到偽裝媒體後，以適當之演算法，即可將機密訊息自偽裝媒體中取出。由於偽裝媒體與掩護媒體幾近相同，故在傳送過程中，即使有心竊密者能取得偽裝媒體，亦無法察覺其內藏有機密訊息，從而達到秘密通訊之目的。藏密學技術更為詳盡之發展背景及相關技術，可參閱 Atawneh, Almomani, and Sumari, (2013)、Cheddad, Condell, Curran, and Mc Kevitt (2010)、Johnson and Jajodia (1998)、Li, He, Huang, and Shi (2011)、Petitcolas, Anderson, and Kuhn (1999)、李榮三、張真誠 (民 98)，以及其內所列出之參考文獻。

評估藏密學技術之優劣有兩個衡量標準(李榮三、張真誠，民 98)：其一是機密訊息之嵌入容量(embedding capacity)；另外則是機密訊息是否容易被偵測察覺。當掩護媒體被嵌入機密訊息成為偽裝媒體後，會造成一定程度之失真，嵌入越多機密訊息，其失真程度越高，亦即偽裝媒體之品質越差。因此，雖然我們希望嵌入容量越大越好，但卻不能造成偽裝媒體之品質過差，而使得有心竊密者察覺偽裝媒體內藏有機密訊息。除了偽裝媒體之品質考量外，另一需考量的問題是，偽裝媒體是否具有特別之特性，而容易被偵測出其內藏有機密訊息。例如，做為掩護媒體之數位影像被嵌入機密訊息後，偽裝影像(stego-image)之直方圖(histogram)是否會有特殊之模式產生，因而使得有心竊密者，能藉由偵測此類模式來判斷數位影像內是否藏有機密訊息。

截至目前為止，已有許多藏密法被提出，而其中有許多是以灰階影像(grayscale image)做為掩護媒體，因就人類視覺系統(human visual system, HVS)而

言，較不易察覺灰階影像像素值(pixel value)之改變。在眾多以灰階影像做為掩護媒體之藏密法中，最廣為人知的應是最不重要位元(least-significant-bit, LSB)取代法(Bender, Gruhl, Morimoto, & Lu, 1996; Chan & Cheng, 2004; Chang, Hsiao, & Chan, 2003; Wang, Lin, & Lin, 2001)。LSB 取代法會將掩護影像每一個像素值固定數量之 LSB，以機密訊息來取代。此種做法的缺點是，人類視覺系統對於影像中平滑區域與複雜區域內之改變，其感知能力並不相同。在平滑區域內之改變，比較容易被人類肉眼察覺，而在複雜區域內之改變，則比較不容易引起注意。因此，若在影像之所有像素皆嵌入相同數量之機密訊息，則在影像之平滑區域內所造成之失真，會比較容易被肉眼所察覺，而知道該影像內藏有機密訊息。為了克服上述 LSB 取代法之缺點，Wu and Tsai (2003)根據 HVS 之特性，提出了像素值差異(pixel-value differencing, PVD)藏密法。PVD 藏密法會根據欲嵌入機密訊息之像素是位於影像之平滑區域或複雜區域中，來決定其機密訊息之嵌入量。位於越平滑區域內之像素，其嵌入之機密訊息量越少，而位於越複雜區域內之像素，其嵌入之機密訊息量則越多，藉此來降低機密訊息被發現的可能性。

由於 PVD 藏密法考慮了 HVS 之特性，因而能降低利用肉眼針對偽裝影像所進行之分析攻擊。在此同時，如 Wu and Tsai (2003)論文中所示，PVD 藏密法亦能抵抗 RS 法(Fridrich, Goljan, & Du, 2001)之攻擊。然而，Zhang and Wang (2004)卻指出，PVD 藏密法所產生之偽裝影像，其像素差值直方圖(pixel difference histogram，以下簡稱 PDH)，會出現不尋常之階梯狀圖形，而使攻擊者能藉此偵知該偽裝影像內藏有機密訊息。尤有甚者，攻擊者甚至能利用 PDH 來推估機密訊息之長度。針對此問題，Zhang and Wang (2004)提出了改良之方法，成功地消除了偽裝影像 PDH 中之階梯狀圖形，使得攻擊者無法藉此來偵知影像內藏有機密訊息。針對 PVD 藏密法之安全性問題，有許多學者提出了改良方法，然而，這些方法均有其缺點，其詳細之說明與比較，可參閱 El-Alfy and Al-Sadi (2012)之評論。

本論文之目的，在於指出，Zhang and Wang (2004)所提出之藏密法，存有先前未曾被發現之瑕疵。此瑕疵與用來將像素差值進行分類之範圍(range)設定有關，由於其不當之範圍寬度設定，在特定情況下，會導致資料嵌入程序(data embedding process)失效，而使其無法實際應用。在此同時，本論文亦將針對該瑕疵，提出改進之方法，以避免嵌入程序失效。

本文之其餘部分組織如下：第貳節介紹 PVD 藏密法與由 Zhang and Wang (2004)所提出之改良方法。在第參節中，將指出 Zhang and Wang (2004)所提出方法之瑕疵，並提出改進之方法。在第肆節中，我們利用測試影像來進行實驗，以驗證本文所提出方法之正確性。第伍節則為結論部分。

貳、PVD 藏密法及其改良

PVD 藏密法包含兩個程序：資料嵌入程序及資料萃取程序(data extraction process)。在資料嵌入程序部分，先以如圖 1 所示之倒 S 形方式掃描掩護影像之像素，並將其以相鄰兩個像素為一組，分割成許多互不重疊之區塊(block)，然後針對每一區塊進行處理。設(x,y)為一區塊中兩個像素之值，其差為 d=y-x。對於 8 位元之灰階影像而言，其像素值之範圍為[0,255]。將[0,255]區分為 n 個連續之範圍 R_i=[l_i,u_i],i=1,⋯,n，且 R_i 之寬度 w_i=u_i-l_i+1，為 2 之冪次。若|d|∈R_k," " k∈{1,⋯,n}，則此區塊可嵌入之訊息量為 log_2⟦(w_k)⟧ 個位元。將 log_2⟦(w_k)⟧ 個位元之機密訊息轉成十進位數 b，並計算

$$d' = \begin{cases} 2^n + b, & 若 d \geq 0 \\ -(2^n + b), & 若 d < 0 \end{cases} \qquad (1)$$

此時|d|及|d^' |會位於相同之 R_k 中，而機密訊息則以下式嵌入此區塊之像素中

$$(x', y') = f(x, y, d') = \begin{cases} (x - \alpha_c, y + \alpha_f), & 若 d 為奇數 \\ (x - \alpha_f, y + \alpha_c), & 若 d 為偶數 \end{cases} \qquad (2)$$

其中 x^'、y^'為嵌入機密訊息後所得到之像素值，α _c=⌈(d^'-d)/2⌉、α _f=⌊(d^'-d)/2⌋，而⌈·⌉與⌊·⌋則分別為天花板函數(ceiling function)與地板函數(floor function)。

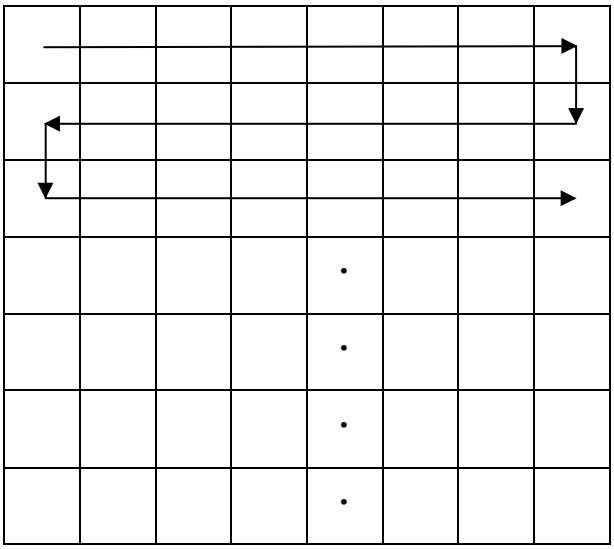


圖 1 倒 S 型掃描方式

在資料萃取程序部分，如同資料嵌入程序之做法，以如圖 1 所示之倒 S 形方式掃描偽裝影像之像素，並將其以相鄰兩個像素為一組，分割成許多互不重疊之區塊。設 x^*及 y^*為一區塊中兩個像素之值，其差為 d^*=y^*-x^*。若|d^* |∈R_k，則嵌於此區塊之機密訊息為 b=|d^* |-l_k。

在嵌入機密訊息後，區塊內之像素值有可能會落於[0,255]之外，亦即出現溢位(overflow)或欠位(underflow)之情況。針對溢位或欠位之情況，PVD 藏密法之處理方式為：在資料嵌入程序部分，設欲處理之掩護影像區塊為(x,y)，且|y-x|∈R_k。

計算(x^,y^)=f(x,y,u_k)。若 x^或 y^落於[0,255]之外，則此區塊予以略過，不嵌入任何機密訊息。而在資料萃取程序部分，設欲處理之偽裝影像區塊為(x^*,y^*)，且|y^*-x^* |∈R_k。計算(x^^*,y^^*)=f(x^*,y^*,u_k)。若 x^^*或 y^^*落於[0,255]之外，則此區塊內並未嵌入機密訊息，予以略過。

PVD 藏密法雖可在靜態影像中嵌入大量機密訊息，並得到品質良好之偽裝影像，同時亦能夠抵抗 RS 分析法之攻擊。然而，其所產生偽裝影像之 PDH，卻會出現不尋常之階梯狀圖形，而使攻擊者可藉此偵測出影像內藏有機密訊息。例如，圖 2a 中之 Lena 影像，其 PDH，如圖 2b 所示，為平滑之圖形。在使用 PVD 藏密法將機密訊息嵌入 Lena 影像後，所得到之偽裝影像，其 PDH 卻會呈現不尋常之階梯狀圖形，如圖 2c 所示。

針對上述 PVD 藏密法之缺點，Zhang and Wang (2004)提出了改良方法，以抵抗藉由分析偽裝影像之 PDH 所進行之攻擊，以提高其安全性，其做法是，在資料嵌入程序部分，選定一金鑰(key)，針對每一區塊，利用此金鑰由虛擬亂數產生器(pseudo-random number generator, PRNG)產生位於[0,1]之參數 β ，然後計算

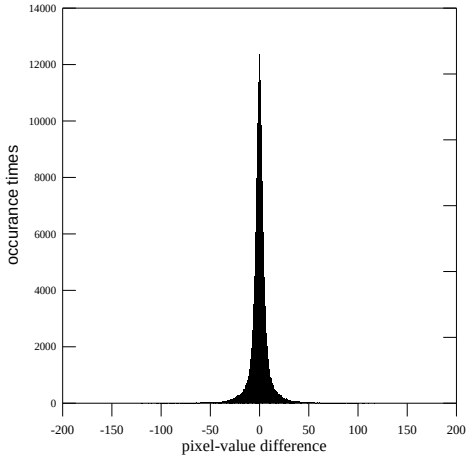
$$\begin{aligned} l'_k &= l_k + \lfloor \beta w_k \rfloor, k = 1, \dots, n \\ u'_k &= l'_{k+1} - 1, k = 1, \dots, n-1 \\ u'_n &= 255 \end{aligned} \qquad (3)$$

若區塊內像素差值之絕對值|d|∈[l_k^',u_k^']," " k∈{1,…,n}，則此區塊可嵌入之訊息量為 log_2⁡〖 (w_k)〗 個位元。將 log_2⁡(w_k)個位元之機密訊息轉成十進位數值 b，並計算

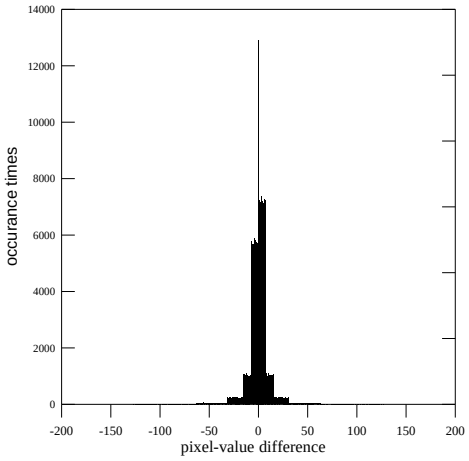
$$d' = \begin{cases} \underset{e \in [-u'_1, u'_1],\ \mathrm{mod}(e, w_1) = b}{\arg\min} |e - d| & \text{若} |d| \in [0, u'_1] \\ \underset{e \in [l'_k, u'_k],\ \mathrm{mod}(e, w_k) = b}{\arg\min} |e - d|, & \text{若} |d| \in [l'_k, u'_k], k \in [2, n] \text{且} d > 0 \\ -\left[\underset{e \in [l'_k, u'_k],\ \mathrm{mod}(e, w_k) = b}{\arg\min} |e + d| \right], & \text{若} |d| \in [l'_k, u'_k], k \in [2, n] \text{且} d < 0 \end{cases} \qquad (4)$$

然後以(2)式將機密訊息 b 嵌入區塊中。

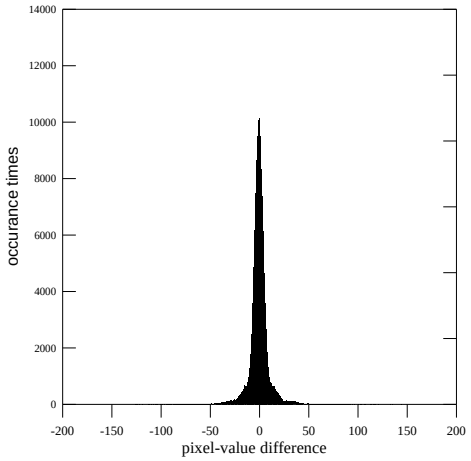
(a)



(b)



(c)



(d)

圖 2： (a) 掩護影像 Lena (b) 掩護影像 Lena 之像素差值直方圖 (c) 使用 PVD 法所產生偽裝影像之像素差值直方圖 (d) 使用 Zhang and Wang 改良法所產生偽裝影像之像素差值直方圖

在資料萃取程序部分，針對每一區塊，利用在資料嵌入程序部分所使用之金鑰，找出嵌入機密訊息時所使用之參數 β，並算出區塊像素差值 d^*之絕對值所在範圍 R_k^'，然後以下式取出嵌於該區塊內之機密訊息 b

$$b = \begin{cases} \mathrm{mod}(d^*, w_1), \text{ 若} |d^*| \in [0, u_1'] \\ \mathrm{mod}(d^*, w_k), \text{ 若} |d^*| \in [l_k', u_k'],\ k \in [2, n] \end{cases} \quad (5)$$

至於在溢位、欠位情況之處理方面，其做法與原 PVD 藏密法之做法相同，惟在嵌入程序中，改為計算 f(x,y,u_k^')而非 f(x,y,u_k)，而在萃取程序中，則改為計算 f(x^*,y^*,u_k^')而非 f(x^*,y^*,u_k)。

利用 Zhang and Wang (2004)提出之改良法，將機密訊息嵌入掩護影像 Lena 後，所得到偽裝影像之 PDH，如圖 2d 所示。由圖 2d 可看出，圖中已不存在不尋常之階梯狀圖形。

參、Zhang and Wang 改良法之修正

雖然 Zhang and Wang (2004)提出之改良法，可有效地去除偽裝影像 PDH 中不尋常之階梯狀圖形，但在特定情況下，其資料嵌入程序卻會失效。例如，設資料嵌入程序使用之連續範圍 R_i," " i=1,⋯,6，其寬度 w_i," " i=1,⋯,6 為 8、8、16、32、64、128。若某一區塊內之像素值為(30,225)，且 β =0.1。因|d|=|225-30|=195，且 l_6^'=128+⌊0.1×128⌋=140、u_6^'=255，故 k=6，而此區塊可嵌入 log_2⟦ (w_6) ⟧ =log_2⟦ (128)=⟧ 7 個位元之機密訊息。由(2)式，因 f(30,225,255)=(0,255)，故嵌入機密訊息後不會產生溢位或欠位。然而，當⟦ e∈[l⟧ _6^',u_6^']時，若機密訊息 b=⟦ 0001010⟧ _2=10，則 mod(e,w_6)=b 無解，無法由(4)式得到 d^'，因而資料嵌入程序失效。事實上，當⟦ e∈[l⟧ _6^',u_6^']時，mod(e,w_6)∈[12,127]。故當 b∈{0,1,⋯,11}時，式(4)無解，資料嵌入程序失效。

要避免(4)式無解而導致資料嵌入程序失效，必須保證當 k∈{1,⋯,n}，且可嵌入區塊之機密訊息量為 m 個位元時，亦即 b∈{0,1,⋯,2^m-1}，至少存在一個整數 e∈[l_k^',u_k^']，使得 mod(e,w_k)=b。Zhang & Wang (2004) 曾指出，因 w_k≤w_(k+1)，由(3)式

$$\begin{aligned} u'_k - l'_k &= l'_{k+1} - 1 - l'_k \\ &= l_{k+1} + \lfloor \beta w_{k+1} \rfloor - 1 - l_k - \lfloor \beta w_k \rfloor \\ &= u_k - l_k + \lfloor \beta w_{k+1} \rfloor - \lfloor \beta w_k \rfloor \\ &= w_k + \lfloor \beta w_{k+1} \rfloor - \lfloor \beta w_k \rfloor \\ &\geq w_k - 1 \end{aligned} \tag{6}$$

故很明顯地，式(4)之解存在。然而，當 k=1,⋯,n-1 時，式(6)的確成立，而(4)式之解存在；但當 k=n 時，因 u_n^'=u_n=255，而

$$\begin{aligned} u'_n - l'_n &= u_n - l_n - \lfloor \beta w_n \rfloor \\ &= w_n - 1 - \lfloor \beta w_n \rfloor \\ &\leq w_n - 1 \end{aligned} \tag{7}$$

故無法保證(4)式之解存在。要保證當 k=n 時(4)式之解存在，w_n 應修正為⟦ w_n^'=u⟧ _n^'-l_n^'+1，此時可嵌入區塊之機密訊息數量為⌊log_2⟦ (w_n^') ⟧ ⌋個位元。至於(4)式，則應修正為

$$d' = \begin{cases} \underset{e\in[-u'_1,u'_1],\ \mathrm{mod}(e,w'_1)=b}{\arg\min} |e-d| & \text{若} |d| \in [0, u'_1] \\ \underset{e\in[l'_k,u'_k],\ \mathrm{mod}(e,w'_k)=b}{\arg\min} |e-d|, & \text{若} |d| \in [l'_k, u'_k], k \in [2,n] \text{且} d>0 \\ -\left[\underset{e\in[l'_k,u'_k],\ \mathrm{mod}(e,w'_k)=b}{\arg\min} |e+d| \right], & \text{若} |d| \in [l'_k, u'_k], k \in [2,n] \text{且} d<0 \end{cases} \tag{8}$$

其中

$$\begin{aligned} w'_k &= w_k, k = 1, \dots, n-1 \\ w'_n &= u'_n - l'_n + 1 \end{aligned} \tag{9}$$

經過修正後，當 k=1,…,n-1 時，式(8)與式(4)相同，故由(6)式，其解必定存在；當 k=n 時，因可嵌入 m^'=⌊log_2⁡〖 (w_n^')〗 ⌋個位元之機密訊息，故 b∈{0,1,…,2^(m^')-1}，且 2^(m^')-1≤w_n^'-1，而由(9)式可知 u_n^'-l_n^'=w_n^'-1，故必存在一個整數 e∈[l_n^',u_n^']，使得 mod(e,w_n^')=b，換句話說，式(8)之解必定存在。

由於(8)、(9)兩式已針對 Zhang and Wang (2004)方法之資料嵌入程序進行修正，故在資料萃取程序部分，為了能正確地萃取出嵌於區塊內之機密訊息，式(5)亦需進行下列修正

$$b=\begin{cases}\mathrm{mod}(d^*,w_1'),\ 若|d^*|\in[0,u_1'] \\ \mathrm{mod}(d^*,w_k'),\ 若|d^*|\in[l_k',u_k'],\ k\in[2,n]\end{cases} \tag{10}$$

其中$w_k', k=1,\dots,n$已定義於(9)式。

在結束本節前，我們以前述導致 Zhang and Wang (2004)方法資料嵌入程序失效之例子來說明上述針對 Zhang and Wang (2004)方法所進行之修正。在資料嵌入程序部分，該像素值為(30,225)之區塊，其可嵌入之機密訊息量，由原先之 7 個位元，修正為⌊log_2⁡〖 (u_6^'-l_6^'+1)〗 ⌋=⌊log_2⁡〖 (255-140+1)〗 ⌋=6 個位元，故機密訊息 b∈{0,1,…,63}。很明顯地，必定存在整數 e∈[l_6^',u_6^']=[140,255]，使得 mod(e,116)=b，因而(8)式之解必定存在，資料嵌入程序不會失效。假設機密訊息 b=〖 001010〗 _2=10，則由(8)式，d^'=242，而由(2)式，嵌入機密訊息後，該區塊之像素值為(6,248)。至於在萃取程序部分，因 d^*=248-6=242∈[l_6^',u_6^']，故 k=6，而由(10)式，萃取出之機密訊息為 b=mod(242,116)=10，與原嵌入之機密訊息相同。

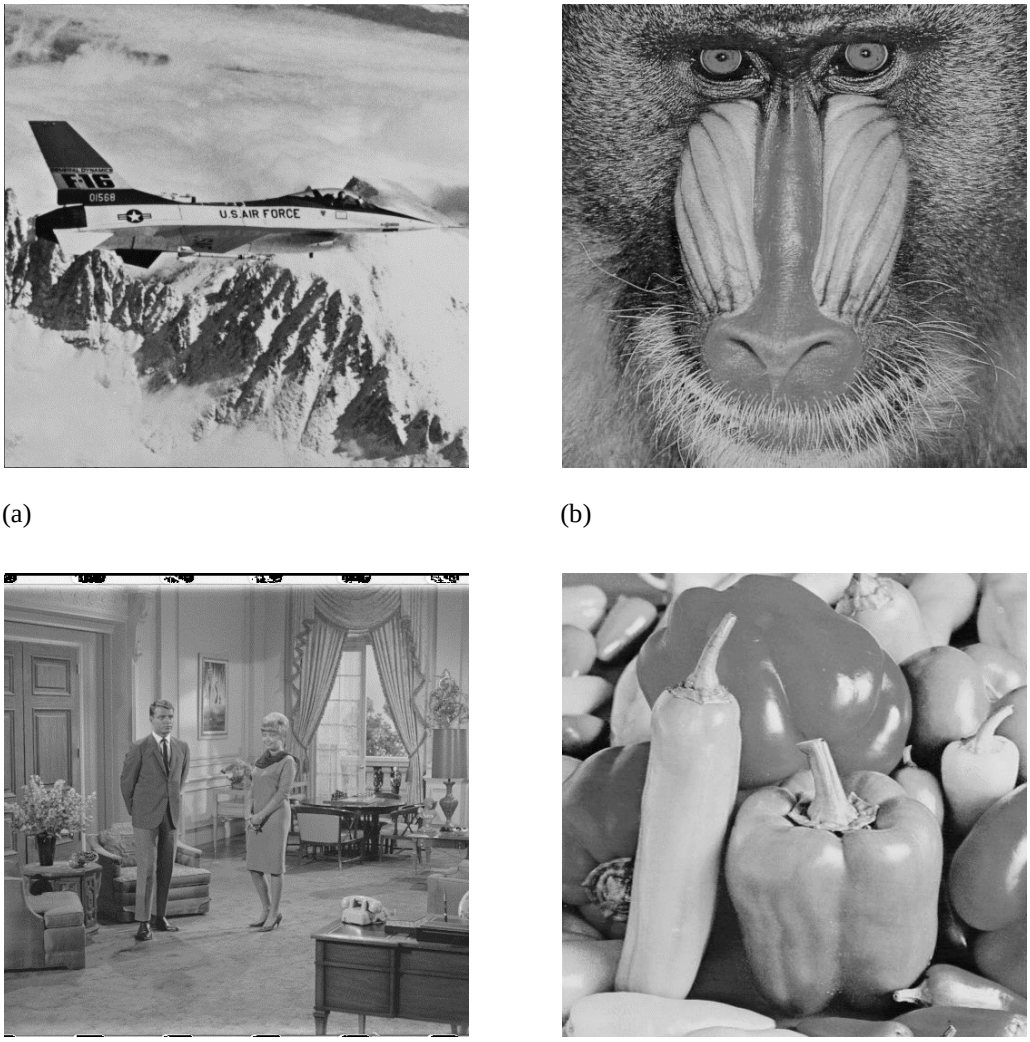
肆、實驗結果

我們以Airplane、Baboon、Couple、Peppers等四張取自USC-SIPI[1]影像資料庫之影像，利用Zhang and Wang (2004)之方法以及本文所提出之方法，將亂數產生之位元流(bit stream)嵌入其中，來進行實驗。此四張影像之大小皆為512x512，且均先轉換為8位元之灰階影像，如圖3所示。

在利用Zhang and Wang (2004)之方法將位元流嵌入圖3中之影像時，Couple影像有38個區塊會導致資料嵌入程序失效，至於Airplane、Baboon、Peppers等影像，則均可成功地嵌入位元流，且資料萃取程序亦可成功地萃取出嵌於其內之位元流。當改以本文所提出之方法來將相同之位元流嵌入影像中時，圖3中之四張影像均可成功嵌入位元流，資料嵌入程序並無失效之情況發生，而嵌於影像中之位元流，亦可成功地利用資料萃取程序萃取出。此結果顯示，本文所提出之方法，的確可成功地解決Zhang and Wang (2004)之方法所存在之資料嵌入程序失效問

[1] http://sipi.usc.edu/database/database.php?volume=misc

題。



(a) (b)

(c) (d)

圖 3 測試影像 (a) Airplane (b) Baboon (C) Couple (D) Peppers

伍、結論

本文指出了Zhang and Wang (2004)所提出之藏密法，存有與用來將像素差值進行分類之範圍設定有關之瑕疵，故其雖可成功地消除由PVD藏密法所得到偽裝影像PDH中，不尋常之階梯狀圖形，但在特定情況下，其資料嵌入程序會失效，而導致其無法實際應用。針對此瑕疵，本文提出了修正之方法，可確保在任何情況下，資料嵌入程序均可成功地將機密訊息嵌入掩護影像中。實驗結果顯示，本文所提出之方法，的確可成功地解決Zhang and Wang (2004)之方法所存在之資料嵌入程序失效問題。

參考文獻

1. 李榮三、張真誠 (民98)。多媒體安全技術之最新發展。載於國家實驗研究院科技政策研究與資訊中心(主編)，**資通安全專論彙編之一**(1-38頁)。台北市：國家實驗研究院。
2. Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. IETE Technical Review, 30(4), 344-358.
3. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35(3-4), 313-336.
4. Chan, C.-K. & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3), 469-474.
5. Chang, C.-C., Hsiao, J.-Y., & Chan, C.-S. (2003). Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36(7), 1583-1595.
6. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: survey and analysis of current methods. *Signal Processing*, 90(3), 727-752.
7. El-Alfy, E.-S. M. & Al-Sadi, A. A. (2012). Pixel-value differencing steganography: attacks and improvements. The Second International Conference on Communications and Information Technology, 757-762.
8. Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color and gray-scale images. IEEE Multimedia Special Issue on Security, 8(4), 22-28.
9. Johnson, N. F. & Jajodia, S. (1998). *Exploring steganography: seeing the unseen. Computer*, 31(2), 26-34.
10. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2(2), 142-172.
11. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). *Information hiding—a survey*. Proceedings of the IEEE, 87(7), 1062-1078.
12. Wang, R.-Z., Lin, C.-F., & Lin, J.-C. (2001). Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognition*, 34(3), 671-683.
13. Wu, D.-C. & Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9-10), 1613-1626.
14. Zhang, X., and Wang, S. (2004). Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. *Pattern Recognition Letters*, 25(3), 331-339.