

植基於預測編碼誤差之無失真影像藏密技術

劉江龍* 李建中

國防大學理工學院電機電子工程學系

摘 要

無失真影像藏密技術在祕密訊息取出後還能將藏密影像回復成原始影像，可提供祕密通訊及影像鑑別的應用。本論文提出以垂直及水平預測誤差方法，創造較高的峰值點統計量，有效改善直方圖位移法藏密量小的缺點。實驗結果顯示，相較於目前基於直方圖的藏密技術，我們提出的方法可大幅提升藏密量，且維持良好藏密影像品質，非常適於軍事影像的藏密應用。

關鍵詞：無失真資訊隱藏，預測編碼，直方圖位移

Lossless Image Steganography Based on Histogram Shifting of Prediction Errors

Chiang-Lung Liu* and Chien-Chung Lee

*Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology,
National Defense University*

ABSTRACT

Lossless image steganography embeds secret data into a digital image and completely restore the original image after removing the hidden data. It is suitable for applications of secure communication and image authentication. In this paper, we propose a novel histogram-based steganographic method which uses prediction errors to create large amount of peak values so that the lower-capacity shortage of histogram-based methods can be improved. Experimental results indicate that the proposed method outperforms the prior works not only in terms of large payload, but also in terms of stego-image quality. Therefore, the proposed method is very suitable for military-image steganographic applications.

Keywords: lossless steganography, predictive coding, histogram shifting

一、前言

隱寫術(Steganography)(也稱為資訊隱藏(Information Hiding)或資料隱藏(Data Hiding))是一種隱匿的通訊技術,起源於軍事情報的傳遞應用,主要作法是將欲傳遞的祕密訊息嵌入掩護載體(Cover Carrier)中,以躲避第三者的察覺,而被嵌入祕密訊息的掩護載體,則通常與欲祕密溝通的訊息無關。接收者在取得藏密的掩護載體後,依所藏密的方法進行逆向的取回程序,以獲得祕密訊息[1]。隱寫術與密碼技術(Cryptography)的作法與要求不同,經密碼技術加密後的訊息通常是無法閱讀,必須以解密金鑰解密後才能閱讀,但加密後的訊息在外觀上呈現無法理解的訊息,容易暴露其祕密通信的意圖,雖難以被第三者破解,但第三者卻可以干擾或破壞祕密通訊的進行;而隱寫術的提出,則是在隱藏祕密通訊的事實,提供另一層次的安全性。在實際應用上,我們會先將欲傳遞的祕密訊息先行加密,再進行隱藏,如此,即使隱藏在掩護載體中的祕密訊息被第三者察覺,亦難以破解[2]。

網際網路是個無遠弗屆的資訊整合環境,多媒體的傳遞與應用因網際網路而蓬勃發展,大量且可輕易取得的多媒體在迅捷便利的網際網路推波助瀾下,提供了資訊隱藏一個絕佳的發展環境[3]。近年來除了祕密通訊外,資訊隱藏技術也盛行於多媒體財產權的保護[4][5],其差別在於,在資訊隱藏的應用中,祕密通訊的作法往往是利用一個普通、易取得、且不易起疑的聲音、文字或影像等數位化多媒體檔案作為媒介,來掩護祕密通訊的進行,訊息傳送者利用藏密演算法將欲傳遞的祕密訊息隱藏於多媒體載體中,再將完成藏密的載體透過公開的管道(例如網際網路)傳遞給接收者;知道藏密演算法的接收者就可以從已藏密的載體中完整的取出祕密訊息,以達到祕密通訊的目的[6]。一個好的資訊隱藏技術通常需滿足強固性(Robustness)、不可察覺性(Imperceptibility)及高藏密量(Capacity)的需求[7],但往往是無法兼顧的[8],而就祕密通訊而言,良好的不可察覺性及高藏密量則是很重要的要求[9][10]。

在眾多的多媒體載體中,數位影像因具有大量散佈、容易取得、及潛存龐大的藏密空間等特性,是最常被利用的傳遞媒介[11],但充

當媒介的載體通常會因藏有祕密訊息而造成影像不可回復的損失,對特殊的運用領域(例如醫學影像或諸如空照或衛星影像等軍事影像)而言,是不允許絲毫破壞的。無失真(Lossless)(或稱可逆式(Reversible)、可回復(Recoverable))的資訊隱藏技術即是在兼顧藏密及原始影像保存的目的下所新興的熱門研究領域,此類研究技術所藏密的影像,在祕密訊息取出後,還能將失真的影像還原成原來的樣子,使得資訊隱藏方法的研究與應用更趨向多元的發展[12]。

發展無失真資訊隱藏技術的關鍵在於一個可以逆向回復的訊息嵌入演算法[13],其演算法主要包括可逆的資訊隱藏演算法及取出與回復原始載體演算法二部分。目前已有很多的學者提出無失真資訊隱藏技術,其可概分為三大類[14]。第一類是利用資料壓縮的技術進行影像特徵值的修改與藏密[15-18];第二類是利用可逆的像素值運算方法進行藏密[19-21];第三類是利用影像像素統計直方圖位移(Histogram Shifting)法進行藏密[22-29]。在第三類方法中,以 Ni 等學者[22]所提出利用直方圖位移法的無失真藏密技術對於影像造成的失真最小,藏密後的影像品質較高,然而卻有藏密量小的缺點。為改善這個缺點,已有學者陸續發展出植基於直方圖位移法的高藏密量技術[24-29]。本論文提出一項可提高直方圖位移藏密量的預測編碼技術,與目前提出基於直方圖之藏密技術比較,在類似的藏密影像品質下,本技術具有更突出的藏密容量表現。為說明本技術,本論文其他段落安排如下:第2節概述各類直方圖位移技術;第3節說明我們提出的方法;第4節為與本技術相關之實驗結果;最後於第5節提出結論。

二、文獻探討

本節探討 Ni 等學者所提出之直方圖位移可逆資訊隱藏技術,並探討其他相關的改進技術。

2.1 Ni 等學者的方法

Ni 等學者於2006年提出直方圖位移可逆資訊隱藏技術,其方法主要是針對載體影像各個像素值的分布次數進行統計,並繪製成直方圖,然後找出直方圖中的峰值點(Peak Point)

及零值點(Zero Point)，藉由峰值點與零值點之間的像素值向零值點方向位移一個像素差值(加 1 或減 1)的方法，挪出鄰近峰值旁的像素值統計空間後，進行秘密訊息的藏入。其藏密及取出與回復的演算法概述於以下各小節。

2.1.1 Ni 等學者的可逆藏密演算法

輸入：原始影像、秘密訊息

輸出：藏密影像、峰值點及零值點

步驟 1：統計原始影像所有像素值並產生直方圖(如圖 1 所示)，隨後從直方圖中找出峰值點 P 及零值點 Z ，並將 P 與 Z 視為金鑰。

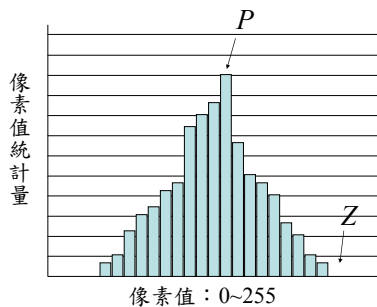


圖 1. 灰階影像像素值直方圖。

步驟 2：依據下列原則將 P 與 Z 間的像素值進行加 1 或減 1 的位移：

- (1)若 $P > Z$ ，則將位於區間 $[Z+1, P-1]$ 的像素值減 1，即減 1 位移。
- (2)若 $P < Z$ ，則將位於區間 $[P+1, Z-1]$ 的像素值加 1，即加 1 位移。

以加 1 位移為例，其位移後的直方圖如圖 2 所示。

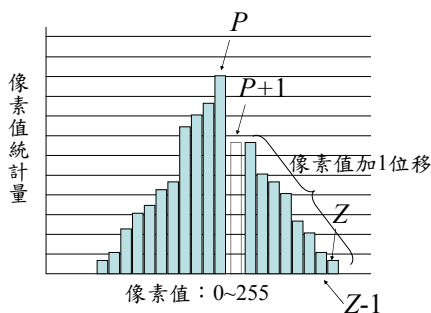


圖 2. 灰階影像像素值位移後之直方圖。

步驟 3：逐一掃描原始影像所有像素，若像素值等於 P ，則依下列原則進行訊息藏密運算：

- (1)當 $P > Z$ ：若藏密訊息位元為 0，像素值不變；若藏入訊息位元為 1，像素值減 1。
- (2)當 $P < Z$ ：若藏密訊息位元為 0，像素值不變；若藏入訊息位元為 1，像素值加 1。

以加 1 位移為例，其藏密後的直方圖如圖 3 所示。

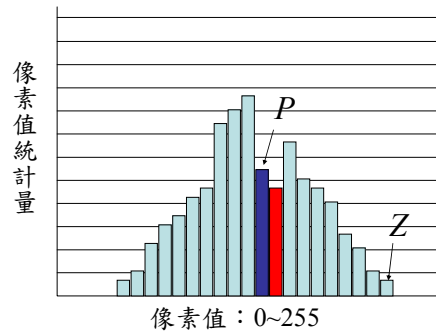


圖 3. 灰階藏密影像像素值直方圖。

2.1.2 Ni 等學者的秘密訊息取出與原始影像回復演算法

輸入：藏密影像、金鑰(即峰值點及零值點)

輸出：原始影像、秘密訊息

步驟 1：統計已藏密影像所有像素值，並產生直方圖。

步驟 2：逐一掃描藏密影像所有像素，若像素值等於 P 、 $P-1$ 或 $P+1$ ，依下列原則取出秘密訊息：

- (1)當 $P > Z$ ：若像素值等於 P ，取出訊息位元 0；若像素值為 $P-1$ ，則取出訊息位元 1，並將像素值加 1。
- (2)當 $P < Z$ ：若像素值等於 P ，取出訊息位元 0；若像素值為 $P+1$ ，則取出訊息位元 1，並將像素值減 1。

步驟 3：依下列原則還原原始影像：

- (1)若 $P > Z$ ，則將位於區間 $[Z, P-2]$ 的像素值加 1。
- (2)若 $P < Z$ ，則將位於區間 $[P+2, Z]$ 的像素值減 1。

在此方法中，若找不到零值點時，則找出最少次數的像素值(稱為低值點(Minimum Point))替代零值點，但基於影像必須還原成原始狀態的要求，這些稱為低值點的像素值所在的位置必須記錄下來，並成為藏密訊息的一部分，一併嵌入載體影像中。

2.2 相關的改進技術

由上一小節的說明可看出，Ni 等學者提出的直方圖位移法的藏密量等於峰值的統計數量。雖然直方圖位移法可重覆進行多次的位移藏密，但影像品質則會隨著藏密次數的增加而逐漸變差。另一種增加藏密量的方法則是採用二組峰值點(即分別向左低值點減 1 或向右低值點加 1 位移)，但採用二組以上的峰值點藏密，就必須慎選零值點，以避免不同峰值組間的位移而造成直方圖重疊，若因無法避免而發生直方圖重疊，則需額外記錄直方圖重疊的像素點資訊以利原始影像的還原，如此將會影響藏密量。然而可預見的是，增加峰值組數或創造高峰值的統計量都是改進直方圖位移法藏密量少缺點的可行方法，因此陸續有學者改進 Ni 學者的方法，提出可創造出高價值統計量與多峰值組的技術。

Fallahpour 等學者[24]於 2007 年提出將影像分割成不重疊的多個區塊，再分別進行位移法藏密，以較多組的峰值點的直方圖位移法提高藏密量。Tseng 等學者[27]則於 2008 年進一步利用影像分割(例如將影像分割成 4×4 個不重疊影像區塊)及每一分割區塊運用 2 組峰值點的方法增加藏密量。其方法是先對每一個影像區塊進行直方圖統計，並在每一個區塊中找到一個峰值點後，各向右及向左位移一個像素值，挪出相鄰峰值點左右二邊的像素值空間便於後續的藏密。藏密時依序掃瞄區塊的像素值，當像素值等於 $P+2$ 且藏入訊息為 0 時，則令像素值不變，當像素值等於 $P+2$ 且藏入訊息為 1 時，則將像素值 $P+2$ 減 1；同理，當像素值等於 $P-2$ 且藏入訊息為 0 時，則令像素值不變，若像素值等於 $P-2$ 且藏入訊息為 1 時，則將像素值 $P-2$ 加 1。此種方法若遇到像素值為 0 或 255 時，則會產生像素值溢位問題(Underflow 或 Overflow)，需記錄還原資訊。

Hong 等學者[28]於 2008 年提出結合預測編碼技術的直方圖位移法，其首先產生一個與

載體大小相同的空的預測矩陣及藏密影像，並將載體影像第一列與第一行的像素值複製到預測矩陣及藏密影像中，然後自第二列及第二行開始依序掃瞄預測矩陣中的像點，利用藏密影像相對位置左上、上方及左方等三個相鄰點的像素值預測右下方位置的像素值，並將預測的像素值與相對原始影像素值相減，得到預測誤差值，並分別在正負方向取 0 及 -1 不同峰值點進行預測誤差值位移藏密，循序完成預測矩陣及藏密影像。若將預測矩陣與原始影像進行像素值的差值運算，可得到一個差值矩陣，Hong 等學者的方法等同於利用直方圖位移法將秘密訊息位元藏在此差值矩陣中，由於差值矩陣具有大量差值為 0 及 -1 的特性，因此可創造出一個較高的峰值點統計量，加上採用二組峰值點進行位移藏密，使其藏密量大增。

Tsai 等學者[29]於 2009 年提出區塊分割的預測編碼直方圖位移法，將影像分割成大小一致(例如 3×3 , 4×4 或 5×5)不重疊區塊，並以位於區塊中間的像素值減去周圍的像素值得到預測誤差值(由於利用影像相鄰像素差異不大的特性，區塊不能分割得太大)，然後分別對每一個區塊進行誤差值的直方圖統計，並分別從正與負的誤差值域中各取一組峰值點，進行直方圖位移法的藏密，大幅的提升了藏密量，就其實驗數據顯示，Tsai 等學者稱其方法平均較 Ni 等學者的方法多達 3 倍的藏密量。

三、我們提出的預測編碼索引技術

在本節中，我們利用上下及左右相鄰像素差異甚微的特性，提出植基於預測誤差的直方圖位移技術，來提升藏密量。由於 Tsai 等學者的預測法以區塊中心點為預測誤差參考值，因此，若區塊設計太大則誤差值無法有效集中；若區塊較小，則需保留較多的預測誤差參考值，而造成峰值統計量的減少。而 Hong 等學者的方法雖然可以達到差值集中的效果，但是其利用藏密影像進行原始影像像素值預測的結果，在影像非平滑地帶會造成較大的預測誤差，影響藏密影像的品質。為改善 Tsai 及 Hong 等學者方法之缺點，我們的方法利用上下或左右相鄰像素的預測誤差值產生預測誤差矩陣，但保留最末列或最末行作為還原預測參考值，利用預測誤差變化甚微的特性創造高價值統計量以增加藏密量，此外，我們是以

原始影像像素值作為參考，以製作預測誤差矩陣，並以預測的像素值進行後續像素值的估測，以避免影響藏密影像品質。本技術先進行垂直方向藏密，再進行水平方向藏密。在垂直方向藏密部分，先將原始影像進行垂直方向的預測編碼，由上向下掃描，每列預測誤差值為目前所在的像素值與下一列像素值的差值，最後保留末列的像素值為還原預測值，並以此組成一預測誤差矩陣，對其進行直方圖統計。接著在預測誤差值的直方圖中分別在正與負的值域中各取一組峰值點與零值點進行直方圖位移藏密。執行完垂直方向藏密之後，接著以此藏密影像進行水平方向藏密，首先依上述原則產生水平方向的預測誤差矩陣，接著進行直方圖統計，同樣在取得二組峰值後，以此水平預測誤差矩陣，進行該藏密影像水平方向的直方圖位移藏密。本文提出的可逆式藏密演算法及取回與回復演算法，詳述於以下各小節。

3.1 我們的可逆式藏密演算法

3.1.1 藏密演算法

輸入：原始影像、秘密訊息。

輸出：藏密影像、4 組峰值點及低值點。

步驟 1：將大小 $m \times n$ 的原始影像 I 進行垂直方向預測編碼。假設 $P(i,j)$ 為原始影像 I 第 (i,j) 位置的像素值， $D_v(i,j)$ 為垂直預測誤差矩陣 D_v 的第 (i,j) 位置的預測誤差值，垂直預測誤差矩陣的計算如下：

$$D_v(i,j) = \begin{cases} P(i,j) - P(i+1,j) & \text{if } 1 \leq i \leq m-1, 1 \leq j \leq n \\ P(i,j) & \text{if } i=m, 1 \leq j \leq n \end{cases} \quad (1)$$

步驟 2：進行垂直預測誤差矩陣直方圖統計。分別取得正、負誤差值域各一組峰值點 $\{V^+, Z^+\}$ 、 $\{V^-, Z^-\}$ ，其中 V^+ 表示正值域的峰值點， Z^+ 表示正值域低值點， V^- 表示負值域的峰值點， Z^- 表示負值域低值點。

步驟 3：進行垂直誤差矩陣直方圖位移。亦即將預測誤差矩陣中誤差值位於區間 $[V^+ + 1, Z^+ - 1]$ 之預測誤差矩陣值加 1 及位於區間 $[Z^- + 1, V^- - 1]$ 之預測誤差矩陣值減 1。位移公式如下：

$$D'_v(i,j) = \begin{cases} D_v(i,j) + 1 & \text{if } V^+ < D_v(i,j) < Z^+ \\ D_v(i,j) - 1 & \text{if } Z^- < D_v(i,j) < V^- \\ D_v(i,j) & \text{otherwise} \end{cases} \quad (2)$$

其中 D'_v 表示變動後之垂直誤差矩陣。
步驟 4：由上而下由左至右順序逐一掃描預測誤差矩陣的所有誤差值，進行垂直預測誤差矩陣 D'_v 的直方圖位移藏密。若誤差值等於 V^+ 或 V^- 時，則進行預測誤差矩陣藏密運算。若欲藏入秘密訊息位元為 0 時，則 V^+ 或 V^- 不變；若秘密訊息位元為 1 時，則將 V^+ 加 1，或將 V^- 減 1，最後得到藏密之垂直預測矩陣 D'_v 。藏密公式如下：

$$D'_v(i,j) = \begin{cases} D'_v(i,j) + 1 & \text{if } D'_v(i,j) = V^+ & \text{and } S = 1 \\ D'_v(i,j) - 1 & \text{if } D'_v(i,j) = V^- & \text{and } S = 1 \\ D'_v(i,j) & \text{if } D'_v(i,j) = V^+ \text{ (or } V^-) & \text{and } S = 0 \end{cases} \quad (3)$$

其中 S 表示欲藏入的秘密訊息位元。
步驟 5：將原始影像 I 之像素值 $P(i+1,j)$ 加上 $D'_v(i,j)$ 值以產生垂直藏密影像 I_v 前 $m-1$ 列之像素值 $P_v(i,j)$ ，並將第 m 列的 $P_v(i,j)$ 值設為 $P(i,j)$ 值，如下式所示：

$$P_v(i,j) = \begin{cases} P(i+1,j) + D'_v(i,j) & \text{if } 1 \leq i \leq m-1, 1 \leq j \leq n \\ P(i,j) & \text{if } i=m, 1 \leq j \leq n \end{cases} \quad (4)$$

步驟 6：進行垂直藏密影像 I_v 水平方向預測編碼。令 $P_v(i,j)$ 為垂直藏密影像 I_v 第 (i,j) 位置的像素值， $D_h(i,j)$ 為水平預測誤差矩陣 D_h 第 (i,j) 位置的預測誤差值，水平預測誤差矩陣的計算如下：

$$D_h(i,j) = \begin{cases} P_v(i,j) - P_v(i,j+1) & \text{if } 1 \leq i \leq m, 1 \leq j \leq n-1 \\ P_v(i,j) & \text{if } 1 \leq i \leq m, j=n \end{cases} \quad (5)$$

步驟 7：進行水平預測誤差矩陣直方圖統計，同時取得正、負誤差值域各一組峰值點 $\{H^+, L^+\}$ 、 $\{H^-, L^-\}$ ，其中 H^+ 表示正值域的峰值點， L^+ 表示正值域低值點， H^- 表示負值域的峰值點， L^- 表示負值域低值點。

步驟 8：進行水平誤差矩陣直方圖位移。亦即將預測誤差矩陣中誤差值位於區間 $[H^+ + 1, L^+ - 1]$ 之預測誤差矩陣值加 1 及位於區間 $[L^- + 1, H^- - 1]$ 之預測誤差矩陣值減 1。位移公式如下：

$$D'_h(i, j) = \begin{cases} D_h(i, j) + 1 & \text{if } H^+ < D_h(i, j) < L^+ \\ D_h(i, j) - 1 & \text{if } L^- < D_h(i, j) < H^- \\ D_h(i, j) & \text{otherwise} \end{cases} \quad (6)$$

其中 D'_h 表示變動後之水平誤差矩陣。

步驟 9：由左至右由上而下順序逐一掃瞄預測誤差矩陣的所有誤差值，進行水平預測誤差矩陣 D'_h 的直方圖位移藏密。若誤差值等於 H^+ 或 H^- 時，則進行預測誤差矩陣藏密運算。若藏入祕密訊息位元為 0 時，則 H^+ 或 H^- 不變；若祕密訊息位元為 1 時，則將 H^+ 加 1 或將 H^- 減 1，最後得到藏密之水平預測誤差矩陣 D'_h 。藏密公式如下：

$$D'_h(i, j) = \begin{cases} D'_h(i, j) + 1 & \text{if } D'_h(i, j) = H^+ & \text{and } S = 1 \\ D'_h(i, j) - 1 & \text{if } D'_h(i, j) = H^- & \text{and } S = 1 \\ D'_h(i, j) & \text{if } D'_h(i, j) = H^+ \text{ (or } H^-) \text{ and } S = 0 \end{cases} \quad (7)$$

步驟 10：將垂直藏密影像 I_v 之像素值 $P_v(i, j+1)$ 加上 $D'_h(i, j)$ 值以產生水平藏密影像 I_h 前 $n-1$ 行之像素值 $P_h(i, j)$ ，並將第 n 行的 $P_h(i, j)$ 值設為相對之 $P_v(i, j)$ 值，如下式所示：

$$P_h(i, j) = \begin{cases} P_v(i, j+1) + D'_h(i, j) & \text{if } 1 \leq i \leq m, 1 \leq j \leq n-1 \\ P_v(i, j) & \text{if } 1 \leq i \leq m, j = n \end{cases} \quad (8)$$

步驟 11：輸出藏密影像 I_h ，並將 4 組峰值點 $\{V^+, Z^+\}$ 、 $\{V^-, Z^-\}$ 、 $\{H^+, L^+\}$ 、及 $\{H^-, L^-\}$ 視為取出密文的金鑰，經由祕密管道傳遞給接收者。

3.1.2 藏密範例

以下我們以一個 5×5 大小的灰階影像為例，說明我們的藏密方法。

步驟 1：假設圖 4 為欲進行可逆資訊隱藏的掩護原始影像 I ，依公式(1)進行垂直方向預測編碼後，得到如圖 5 之垂直預測誤差矩陣 D_v 。

步驟 2：將垂直預測誤差矩陣進行直方圖統計，並選取正負誤差值域中二組峰值點 $\{0, 2\}$ 及 $\{-1, -2\}$ 。

步驟 3：依公式(2)將誤差為 1 的值加 1 以進行直方圖位移(誤差值由 1 位移到 2)；另外，因負的誤差值存在僅峰值點 -1 ，因此不需進行位移，位移後之垂直預

測誤差矩陣統計直方圖如圖 6 所示。

步驟 4：由上往下由左至右掃瞄 D_v ，當預測誤差值等於 0 或 -1 時，依公式(3)進行藏密：

(1)當祕密訊息位元為 0 時，預測誤差值不變。

(2)當祕密訊息位元為 1 時，若預測誤差值為 -1 ，則預測誤差值減 1，若預測誤差值為 0，則預測誤差值加 1。

最後完成如圖 7 之垂直藏密預測誤差矩陣影像 D'_v 。

步驟 5：依公式(4)得到垂直藏密影像 I_v ，如圖 8 所示。

步驟 6：依公式(5)將垂直藏密影像 I_v 進行水平預測編碼，得到如圖 9 之水平預測誤差矩陣 D_h 。

步驟 7：將水平預測誤差矩陣進行直方圖統計，並選取正負誤差值域中二組峰值點 $\{0, 3\}$ 及 $\{-2, -3\}$ ，如圖 10 所示。

步驟 8：依公式(6)將誤差值位於區間 $[1, 3]$ 之誤差值加 1 以進行向右位移(誤差值 1 至 2 位移到 2 至 3)；另外，因負的峰值 -2 左邊無其他統計值，因此不需進行向左位移。

步驟 9：由左往右由上至下掃瞄 D_h ，當誤差值等於 0 或 -2 時，依公式(7)進行藏密：

(1)當祕密訊息位元為 0 時，預測誤差值不變。

(2)當祕密訊息位元為 1 時，若誤差值為 -2 ，則誤差值減 1，若誤差值為 0，則誤差值加 1。

最後完成如圖 11 之水平藏密預測誤差矩陣影像 D'_h 。

步驟 10：依公式(8)得到水平藏密影像 I_h ，如圖 12 所示。

步驟 11：輸出水平藏密影像 I_h 及四組峰值點 $\{0, 2\}$ 、 $\{-1, -2\}$ 、 $\{0, 3\}$ 、 $\{-2, -3\}$ 。

	j					
	1	2	3	4	5	
i	1	178	178	179	178	179
	2	179	178	179	178	178
	3	179	178	179	178	178
	4	179	178	178	178	178
	5	180	179	179	179	179

圖 4. 原始影像 I 。

密文位元串
0101 0001 110 1011 011

藏密順序	0	178	0	178	1	180	1	179	180
	1	180	0	178	1	180	0	178	0
	0	179	0	178	180	1	179	1	179
	1	178	1	177	0	178	1	177	1
	180	179	179	179	179	179	179	179	179

圖 8. 垂直藏密影像 I_v 。

須位移(+1)

-1	0	0	0	1
0	0	0	0	0
0	0	1	0	0
-1	-1	-1	-1	-1
180	179	179	179	179

圖 5. 影像 I 之垂直預測誤差矩陣 D_v 。

須位移(+1)

0	-2	1	-1	180
2	-2	2	0	178
1	-2	1	0	179
1	-1	1	0	177
1	0	0	0	179

圖 9. 影像 I_v 之水平預測誤差矩陣 D_h 。

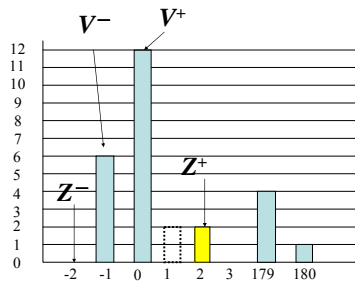


圖 6. 位移後之垂直預測誤差統計直方圖。

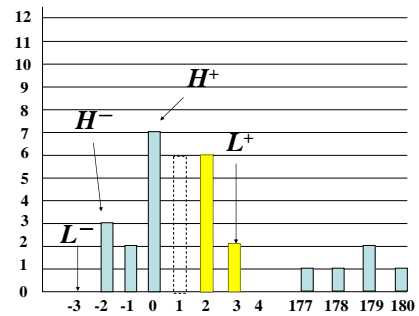


圖 10. 位移後之水平預測誤差統計直方圖。

密文位元串
0101 0001 110 1011 011

藏密順序	0	-1	0	0	1	1	1	2
	1	1	0	0	1	1	0	0
	0	0	0	0	2	1	1	1
	1	-2	1	2	0	-1	1	-2
	180	179	179	179	179	179	179	179

圖 7. 垂直藏密預測誤差矩陣 D'_v 。

密文位元串
01 11 01 0 101

藏密順序	0	0	1	-3	2	-1	180
	3	1	-3	3	1	1	178
	2	0	-2	2	1	1	179
	2	-1	2	0	0	0	177
	2	1	0	0	1	1	179

圖 11. 水平藏密預測誤差矩陣 D'_h 。

密文位元串
01 11 01 0 101

藏密順序

	0	178		1	177		181		179		180

圖 12. 水平藏密影像 I_h 。

3.2 我們的取出及回復演算法

3.2.1 取出及回復演算法

我們的秘密訊息取出及回復程序是採取與藏密程序逆向的順序，逐一取出訊息位元並同時回復該像素值的步驟進行。詳細之取出與回復演算法如下：

輸入：藏密影像 I_h 及 4 組峰值點。

輸出：秘密訊息及原始影像。

步驟 1：依據水平藏密影像 I_h 第 n 行之像素值 $P_h(i, j)$ 還原垂直藏密影像 I_v 第 n 行之像素值 $P_v(i, j)$ ，亦即：

$$P_v(i, j) = P_h(i, j), \quad 1 \leq i \leq m, \quad j = n \quad (9)$$

步驟 2：將水平藏密影像進行由右向左由下而上的逆向水平順序逐一取出秘密訊息及還原水平預測誤差值 $D_h(i, j)$ ，並據以還原前 $n-1$ 行之垂直藏密影像之像素值：

(1) 依下式計算水平藏密影像位移後之第 (i, j) 位置的預測誤差值 $D'_h(i, j)$ ：

$$D'_h(i, j) = P_h(i, j) - P_v(i, j+1) \quad (10)$$

(2) 若 $D'_h(i, j)$ 等於 H^+ 、 $H^+ + 1$ 、 H^- 及 $H^- - 1$ 時，則執行公式(11)以取出秘密訊息 S ，並執行公式(12)以還原水平預測誤差值 $D_h(i, j)$ ：

$$S = \begin{cases} 0, & \text{if } D'_h(i, j) = H^+ \quad \text{or } H^- \\ 1, & \text{if } D'_h(i, j) = H^+ + 1 \quad \text{or } H^- - 1 \end{cases} \quad (11)$$

$$D_h(i, j) = \begin{cases} D'_h(i, j) - 1 & \text{if } D'_h(i, j) = H^+ + 1 \\ D'_h(i, j) + 1 & \text{if } D'_h(i, j) = H^- - 1 \end{cases} \quad (12)$$

(3) 若 $D'_h(i, j)$ 位於區間 $[H^+ + 2, L^+]$ ，則將 $D'_h(i, j)$ 減 1；若 $D'_h(i, j)$ 位於區間 $[L^-, H^- - 2]$ ，則將 $D'_h(i, j)$ 加 1，以還原水平預測誤差值 $D_h(i, j)$ 。如下式所示：

$$D_h(i, j) = \begin{cases} D'_h(i, j) - 1 & \text{if } H^+ + 1 < D'_h(i, j) < L^+ + 1 \\ D'_h(i, j) + 1 & \text{if } L^- - 1 < D'_h(i, j) < H^- - 1 \\ D'_h(i, j) & \text{otherwise} \end{cases} \quad (13)$$

(4) 依下式回復垂直藏密影像之像素值 $P_v(i, j)$ ：

$$P_v(i, j) = P_v(i, j+1) + D_h(i, j) \quad (14)$$

步驟 3：依據垂直藏密影像第 m 列之像素值 $P_v(i, j)$ 還原原始影像 I 第 m 列之像素值 $P(i, j)$ ，亦即：

$$P(i, j) = P_v(i, j), \quad i = m, \quad 1 \leq j \leq n \quad (15)$$

步驟 4：將垂直藏密影像進行由下而上由右至左的逆向垂直順序逐一取出秘密訊息及還原垂直預測誤差值 $D_v(i, j)$ ，並據以還原前 $m-1$ 列之原始影像像素值：

(1) 依下式計算垂直藏密影像位移後之第 (i, j) 位置的預測誤差值 $D'_v(i, j)$ 。

$$D'_v(i, j) = P(i, j) - P_v(i+1, j) \quad (16)$$

(2) 若 $D'_v(i, j)$ 等於 V^+ 、 $V^+ + 1$ 、 V^- 及 $V^- - 1$ 時，則執行公式(17)以取出秘密訊息 S ，並執行公式(18)以還原垂直預測誤差值 $D_v(i, j)$ ：

$$S = \begin{cases} 0, & \text{if } D'_v(i, j) = V^+ \quad \text{or } V^- \\ 1, & \text{if } D'_v(i, j) = V^+ + 1 \quad \text{or } V^- - 1 \end{cases} \quad (17)$$

$$D_v(i, j) = \begin{cases} D'_v(i, j) - 1 & \text{if } D'_v(i, j) = V^+ + 1 \\ D'_v(i, j) + 1 & \text{if } D'_v(i, j) = V^- - 1 \end{cases} \quad (18)$$

(3) 若 $D'_v(i, j)$ 位於區間 $[V^+ + 2, Z^+]$ ，則將 $D'_v(i, j)$ 減 1，若 $D'_v(i, j)$ 位於區間 $[Z^-, V^- - 2]$ ，則將 $D'_v(i, j)$ 加 1，以還原垂直預測誤差值 $D_v(i, j)$ 。如下式所示：

$$D_v(i, j) = \begin{cases} D'_v(i, j) - 1 & \text{if } V^+ + 1 < D'_v(i, j) < Z^+ + 1 \\ D'_v(i, j) + 1 & \text{if } V^- - 1 < D'_v(i, j) < Z^- - 1 \\ D'_v(i, j) & \text{otherwise} \end{cases} \quad (19)$$

(4)依下式回復原始影像之像素值 $P(i, j)$:

$$P(i, j) = P(i + 1, j) + D_v(i, j) \quad (20)$$

步驟 5：輸出原始影像 I ，並將所有取出的秘密訊息位元收集成秘密位元串，以利後續秘密訊息的解密。

3.2.2 取出及回復範例

以下我們仍以上一小節的藏密範例說明取出秘密訊息及回復的過程。首先輸入水平藏密影像 I_h (如圖 13 之左圖所示)及四組峰值點 $\{0, 2\}$, $\{-1, -2\}$, $\{0, 3\}$, $\{-2, -3\}$ 。

步驟 1：依公式(9)將水平藏密影像最後一行之像素值複製到欲還原之垂直藏密影像最後一行，如圖 13 之步驟 1 所示。

步驟 2：依公式(10)-(14)將水平藏密影像 I_h 前 4 行個別像素進行由右至左由下向上的逆向水平順序取出秘密訊息及還原垂直藏密影像 I_v 。

以水平藏密影像第(5,4)像素為例，其秘密訊息取出與還原順序如下：

(1)依公式(10)得到位移後之預測誤差值 $D'_h(5,4) = P_h(5,4) - P_v(5,5) = 180 - 179 = 1$ 。

(2)依公式(11)取出秘密訊息 $S=1$ (因為 $H^+ + 1 = 1$)。

(3)依公式(12)還原位移前之預測誤差值 $D_h(5,4) = D'_h(5,4) - 1 = 0$ (因為 $D'_h(5,4) = H^+ + 1$)。

(4)依公式(14)還原垂直藏密影像之像素值 $P_v(5,4) = P_v(5,5) + D_h(5,4) = 179 + 0 = 179$ 。

已知 $P_h(5,3)$ 與求得之 $P_v(5,4)$ ，則可繼續取得隱藏在 $P_h(5,3)$ 像素值之秘密訊息，及還原垂直藏密影像 $P_v(5,3)$ 之像素值。依此類推，即可將隱藏在水平藏密影像之秘密訊息全部取出及還原垂直藏密影像 I_v (如圖 14 左圖所示)。

步驟 3：依公式(15)將垂直藏密影像最後一列之像素值複製到欲還原之原始影像

最後一列，如圖 14 之步驟 3 所示。

步驟 4：依公式(16)-(20)將垂直藏密影像 I_v 前 4 列個別像素進行由下而上由右至左的逆向垂直順序取出秘密訊息及還原原始影像 I 。

以垂直藏密影像第(4,5)像素為例，其秘密訊息取出與還原順序如下：

(1)依公式(16)得到位移後之預測誤差值 $D'_v(4,5) = P_v(4,5) - P(5,5) = 177 - 179 = -2$ 。

(2)依公式(17)取出秘密訊息 $S=1$ (因為 $V^- - 1 = -2$)。

(3)依公式(18)還原位移前之預測誤差值 $D_v(4,5) = D'_v(4,5) + 1 = -1$ (因為 $D'_v(4,5) = V^- - 1$)。

(4)依公式(20)還原垂直藏密影像之像素值 $P(4,5) = P(5,5) + D_v(4,5) = 179 + (-1) = 178$ 。

已知 $P_v(3,5)$ 與求得之 $P(4,5)$ ，則可繼續取得隱藏在 $P_v(3,5)$ 像素值之秘密訊息，及還原原始影像 $P(3,5)$ 之像素值。依此類推，即可將隱藏在垂直藏密影像之秘密訊息全部取出及還原原始影像 I 。

步驟 5：輸出原始影像 I ，並將所有取出的秘密訊息位元收集成秘密位元串 $\{010100011101011011, 011101010101\}$ ，以利後續秘密訊息的解密。

四、實驗結果

為證明本無失真藏密技術的有效性，我們使用 6 張 512×512 大小的灰階測試影像(如圖 15 所示)作為原始影像，並以同一個亂數種子隨機產生位元串流模擬秘密訊息，以進行藏密、萃取及還原實驗，藏密影像品質並以信號雜訊比(PSNR, Peak Signal to Noise Ratio)作為評量的標準，其計算方式如下：

$$PSNR = 10 \times \log \left(\frac{255^2}{MSE} \right) \text{ (dB)} \quad (21)$$

其中 MSE 為均方差(Mean Square Error)，計算公式如下：

$$MSE = \left(\frac{1}{m^2} \right) \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (\alpha_{ij} - \beta_{ij})^2 \quad (22)$$

其中 α_{ij} 表示原始影像在 (i, j) 位置的像素值， β_{ij} 為藏密影像在 (i, j) 位置的像素值。信號雜訊比值越高，表示影像因藏密後的破壞越小，一般可以被人類視覺系統接受的信號雜訊比需要大於 30 dB。

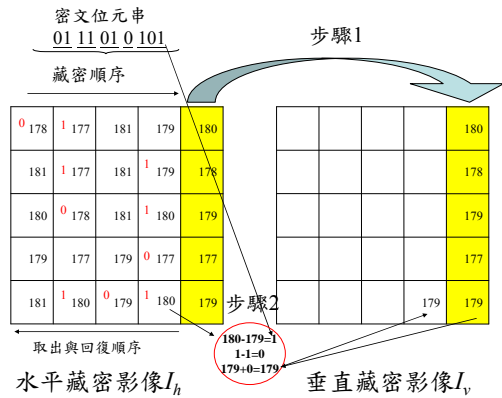


圖 13. 取出及回復第(5,4)位置像素值的範例。

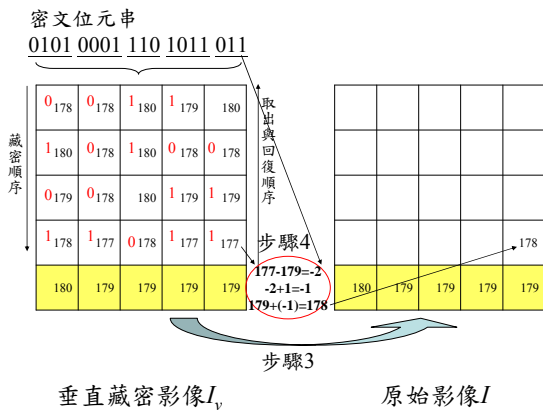


圖 14. 取出及回復第(4,5)位置像素值的範例。



圖 15. 六張測試影像。

4.1 我們的方法在不同峰值點選擇法的藏密效果

為避免利用多組的峰值點造成重疊的情況，我們先在垂直或水平方向分別取二組峰值點進行單方向藏密，接著在垂直及水平方向各取一組峰值點進行藏密，再接著在垂直與水平方向各取二組峰值點(合計 4 組)進行藏密實驗，上述實驗結果如表 1 所示。

從表 1 可以看出，若只取兩組峰值點，則在垂直方向採用負向零值點及在水平方向採用正向零值點的作法所產生的偽裝影像品質最好，此時平均藏密量約為 88223 位元，藏密影像品質可達 51 dB。一般而言，在取二組峰值點情形下，藏密影像的品質均能保持 48 dB 以上。此外，因相鄰像素之像素值相似，而有預測誤差值較小且向零集成的特性，我們從實驗中發現，不論是先水平後垂直或先垂直後水平進行藏密所產生的預測誤差矩陣，其零均為峰值點，顯示可重複運用相鄰像素的零誤差值所創造出來的高統計量，來進行直方圖位移藏密。因此在垂直預測藏密及水平預測藏密中均採用二組峰值點進行藏密後，藏密量平均提高約一倍，且藏密影像品質平均仍可維持 45 dB 以上。

4.2 我們的方法與其他方法的比較

為證明我們所提方法的優越性，我們同時進行與其他學者所提方法的效能比較實驗。為求客觀，所有測試的實驗方法均採用二組峰值點，並以同一個亂數種子隨機產生位元串流來模擬秘密訊息，實驗結果如表 2 所示。

表 1. 我們的方法在不同峰值點選擇法之實驗結果

影像	垂直預測取二組峰值點		水平預測取二組峰值點		垂直取右、水平取左各一組峰值點		垂直取左、水平取右各一組峰值點		垂直與水平預測各取二組峰值點	
	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)
Lena	109158	49.16	83136	50.94	76473	50.76	115860	50.97	181400	45.89
Boat	84594	48.91	84465	50.68	81879	50.57	84413	51.02	154892	44.89
F16	101348	49.09	111216	50.78	105190	50.85	110931	51.08	196834	45.97
Pepper	83081	48.89	80836	50.84	77208	50.84	82078	50.96	155184	45.93
Tiffany	83075	48.95	76748	50.68	77632	50.73	78246	51.09	162230	45.94
Barbara	60936	48.68	51165	50.76	52277	50.39	57808	51.01	106338	45.66
平均	87032	48.95	81261	50.78	78443.16	50.69	88222.67	51.02	159479.67	45.71

表 2. 我們的方法與其他方法比較結果

影像	Ni		Fallahpour		Tseng		Hong		Tsai		我們的方法	
	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)	實際藏密度 (位元)	PSNR (dB)
Lena	5700	49.34	8591	50.3	10230	48.37	88752	48.96	71351	49.1	115860	50.97
Boat	10898	48.22	12940	50.69	20623	48.54	76933	48.84	65520	49.04	84413	51.02
F16	19151	48.38	20572	49.34	15442	48.62	90991	48.99	83998	49.23	110931	51.08
Pepper	5072	51.31	8425	50.09	13083	48.36	93604	49.01	55857	48.94	82078	50.96
Tiffany	9004	48.21	12999	51.66	15318	48.51	88976	49.02	56374	49.01	78246	51.09
Barbara	4722	48.21	6625	49.48	9649	48.31	62572	48.71	40795	48.79	57808	51.01
平均	9091.17	48.95	11692	50.26	14057.5	48.45	83638	48.92	62315.83	49.02	88222.67	51.02

從表 2 可看出，平均而言，我們的方法較其他學者的方法擁有較佳的藏密度，且較 Tsai 等學者於 2009 年所提的方法高出將近一倍；而 Hong 等學者的方法所產生的預測誤差具有向零集中效果，已大幅改善一般利用影像像素值直方圖位移法藏密度低的缺點，而我們提出的方法的藏密度則與其相當，但擁有較佳的藏密影像品質。

特別一提的是，在所有基於預測編碼的藏密技術中，由於預測誤差可能為正值或負值，若位移的像素值或藏密的像素值是 0 或 255 時，難免會產生像素值溢位的問題，當位移或欲藏入密文的像素值為 0 或 255 時我們並不處理(不位移或藏密)，並記錄該像素值的位置資訊，連同祕密訊息藏入偽裝影像中，以利後續的原始影像還原。但在我們的實驗中這種情況是不多的，例如我們選用的測試影像中，僅 F16 及 Tiffany 這二張影像會對 Tseng、Hong、Tsai 等學者及我們的方法造成溢位情形，例如 Tsai 學者的方法共有 103 個像素溢位，我們的

方法採用二組峰值點會有個 322 個像素溢位，四個峰值點則有 992 個像素溢位，若以 512×512 大小的影像為例，記錄一個像素值的位置(i,j)共需 18 個位元，表 1 及表 2 的藏密度實驗數據均為已扣除額外資訊的實際藏密度，從實驗數據可知，平均而言，在所有比較的方法中，我們的方法具有最高的實際藏密度，且具有更好的視覺品質。

上述之實驗結果進一步分析如下：

- (1) 在直方圖位移法中，不論挪出藏密空間(簡稱挪移)或進行峰值的藏密位移(簡稱位移)，都會造成影像失真。峰值統計量越高，表示挪移的像素值較少；另外，因藏密位移的機率為 1/2(訊息位元為 1 時才位移)，峰值統計量越高，同時表示不用進行位移的像素值愈多。因此，若擁有較高峰值統計量，除了藏密度較大外，也將擁有較高的藏密影像品質。我們的方法利用上下或左右相鄰像素值相近的特性，採用上下或左右預測誤差值進行藏密，以創造比

其他方法高的峰值統計量。因此，我們的方法在具有高密量的同時，也具備良好的藏密影像品質。

- (2) 以預測編碼法為基礎的無失真藏密技術需保留足夠多的還原參考值以達到可逆的資訊隱藏，但保留太多還原參考值亦將減少峰值的統計量。例如，Tsai 等學者將影像分割成不重疊區塊，並保留區塊中心點作為還原參考值，因此保留了較多的還原參考值，影響峰值統計量。我們所提的方法僅保留一行(水平藏密)或一列(垂直藏密)的還原參考值，且水平及垂直藏密交替藏密後，具有修正像素值誤差的效果，因此，與其他以預測編碼法為基礎的無失真藏密技術相比，我們的方法除擁有較高的峰值統計量，且具有良好藏密影像品質。

4.3 實驗討論

對以預測編碼法為基礎的無失真藏密技術而言，若不加以限制峰值點及零值點取的方向，則可能發生正的預測誤差值的峰值點落在零值點的右方或負的預測誤差值的峰值點落在零值點的左方現象。但一般來說，由於預測誤差值的統計分布會向零集中，這種現象不容易出現。以我們的方法為例，影像 Lena 的水平誤差矩陣統計直方圖如圖 16 所示，二組正負峰值一般非常靠近且趨近於零，也就是說，其正值域的零值點必在峰值點的右側(即 $H^+ < L^+$)，且負值域的零值點必在峰值點的左側(即 $L^- < H^-$)，此為本方法只討論 $H^+ < L^+$ 及 $L^- < H^-$ (或 $V^+ < Z^+$ 及 $Z^- < V^-$) 情況的原因。為了單純化，在實際應用上，我們的方法會限定 $H^+ < L^+$ 及 $L^- < H^-$ (或 $V^+ < Z^+$ 及 $Z^- < V^-$)。

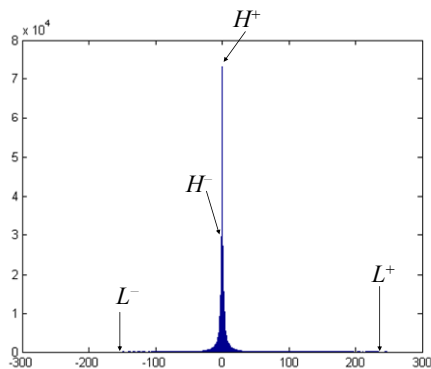


圖 16. 影像 Lena 的水平誤差矩陣統計直方圖。

五、結論

本論文提出一種基於直方圖位移的無失真藏密技術，本技術利用相鄰像素預測編碼法分別求得垂直及水平預測誤差矩陣，並以該誤差矩陣進行直方圖位移藏密。我們的方法利用相鄰像素相似的特性，所求得的預測誤差值較小且向零集中，可創造較高的峰值統計量，大幅提升藏密量，此外，我們是以原始影像像素值作為參考以製作預測誤差矩陣，並非以藏密影像的像素值進行後續像素值的估測，因此不會造成預測誤差值遞延漸增的問題，可維持很好的藏密影像品質。實驗結果顯示，我們的方法在以直方圖位移法為基礎的可逆藏密技術中，擁有較好的藏密效能，非常適用於醫學或軍事影像的應用。

參考文獻

- [1] Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G., "Information Hiding-A Survey," Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062-1078, Jul. 1999.
- [2] Rabah, K., "Steganography-The Art of Hiding Data," Information Technology Journal, Vol. 3, No. 3, pp. 245-269, 2004.
- [3] Lou, D.-C. and Liu, J.-L., "Steganographic Method for Secure Communications," Computers and Security, Vol. 21, No. 5, pp. 449-460, Oct. 2002.
- [4] Grover, D., "Steganography for Identifying Ownership of Copyright," Computer Law & Security Report, Vol. 14, No. 2, pp. 121-122, Mar. 1998.
- [5] Yeung, M. M. and Mintzer, F., "An Invisible Watermarking Technique for Image Verification," Proceedings of IEEE International Conference on Image Processing, Vol. 2, Santa Barbara, CA, pp. 680-683, Oct. 1997.
- [6] Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., and Shamsuddin, M. Z. I., "Information Hiding Using Steganography," Proceedings of 4th National Conference on Telecommunication Technology, pp. 21-25, Jan. 2003.
- [7] Cacciaguerra, S. and Ferretti, S. "Data Hiding: Steganography and Copyright

- Marking,”
http://www.cs.unibo.it/~scacciag/home_files/teach/datahiding.pdf
- [8] Bender, W., Gruhl, D., Morimoto, N., and Lu, A., “Techniques for Data Hiding,” *IBM System Journal*, Vol. 35, No. 3&4, pp. 313-336, 1996.
- [9] Liao, Z., Huang, Y., and Li, C., “Research on Data Hiding Capacity,” *International Journal of Network Security*, Vol. 5, No. 2, pp. 140-144, Sep. 2007.
- [10] Wu, N.-I. and Hwang, M.-S., “Data Hiding: Current Status and Key Issues,” *International Journal of Network Security*, Vol. 4, No. 1, pp. 1-9, Jan. 2007.
- [11] Duke, D., “Image Is Everything,” *Network Security*, Vol. 2002, No. 4, pp. 4-5, Apr. 2002.
- [12] Huang, H.-C., Huang, Y.-H., Pan, J.-S., and Lu, Y.-Y., “Information Protection and Recovery with Reversible Data Hiding,” *Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Vol.2, pp. 461-464, Nov. 2007.
- [13] Awrangjeb, M., “An Overview of Reversible Data Hiding,” *Proceedings of the 6th International Conference on Computer and Information Technology (ICCIT-03)*, Dhaka, Bangladesh Dhaka, Bangladesh, pp. 75-79, Dec. 2003.
- [14] Feng, J.-B., Lin, I.-C., Tsai, C.-S., and Chu, Y.-P., “Reversible Watermarking: Current Status and Key Issues,” *International Journal of Network Security*, Vol. 2, No. 3, pp. 161-171, May 2006.
- [15] Chang, C.-C., Hsiao, J.-Y., and Chan, C.-S., “Finding Optimal Least-significant-bit Substitution in Image Hiding by Dynamic Programming Strategy,” *Pattern Recognition*, Vol. 36, No. 7, pp. 1583-1595, Jul. 2003.
- [16] Celik, M. U., Sharma, G., Tekalp, A. M., and Saber, E., “Lossless Generalized-LSB Data Embedding,” *IEEE Transactions on Image processing*, Vol. 14, No. 2, pp. 253-266, Feb. 2005.
- [17] Chang, C.-C., Lin, C.-C., Tseng, C.-S., and Tai, W.-L., “Reversible Hiding in DCT-based Compressed Images,” *Information Sciences*, Vol. 177, No. 13, pp. 2768-2786, Jul. 2007.
- [18] Hong, W., Chen, T.-S., and Shiu, C.-W., “Lossless Steganography for AMBTC-Compressed Images,” in *Congress on Image and Signal Processing*, Vol. 2, pp. 13-17, May 2008.
- [19] Vleeschouwer, C. D., Delaigle, J. F., and Macq, B., “Circular Interpretation of Bijective Transformation in Lossless Watermarking for Media Asset Management,” *IEEE Transactions on Multimedia*, Vol. 5, No. 1, pp. 97-105, Mar. 2003.
- [20] Tian, J., “Reversible Data Embedding and Content Authentication Using Difference Expansion,” *IEEE Transaction on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 831-841, Aug. 2003.
- [21] Alattar, A. M., “Reversible Watermark Using the Difference Expansion of A Generalized Integer Transform,” *IEEE Transactions on Image Processing*, Vol. 13, No. 8, pp. 1147-1156, Aug. 2004.
- [22] Ni, Z., Shi, Y. Q., Ansari, N., and Su, W., “Reversible Data Hiding,” *IEEE Transactions on Circuits and Systems for Video Technology*, Vol.16, No. 3, pp. 354-362, Mar. 2006.
- [23] Xuan, G. et al., “Lossless Data Hiding Using Histogram Shifting Method Based on Integer Wavelets,” *Proceedings of International Workshop on Digital Watermarking*, pp. 323-332, Nov. 2006.
- [24] Fallahpour, M. and Sedaaghi, M. H., “High Capacity Lossless Data Hiding Based on Histogram Modification,” *IEICE Electronics Express*, Vol. 4, No. 7, pp. 205-210, 2007.
- [25] Chrysochos, E., Fotopoulos, V., Skodras, A., and Xenos, M., “Reversible Image Watermarking Based on Histogram Modification,” *Proceedings of the 11th Panhellenic Conference on Informatics with International Participation (PCI 2007)*, Vol. B, pp. 93-104, May 2007.
- [26] Kim, K.-S., Lee, M.-J., Lee, H.-K., and Suh, Y.-H., “Histogram-Based Reversible Data Hiding Technique Using Subsampling,” *Proceedings of the 10th ACM workshop on Multimedia and Security*, pp. 69-74, 2008.
- [27] Tseng, H.-W. and Hsieh, C.-P., “Reversible Data Hiding Based on Image Histogram Modification,” *Imaging Science Journal*,

- Vol. 56, No. 5, pp. 271-278, Oct. 2008.
- [28] Hong, W., Chen, T.-S., and Shiu, C.-W.,
“Reversible Data Hiding Based on
Histogram Shifting of Prediction Errors,”
Proceedings of International Symposium on
Intelligent Information Technology
Application Workshops 2008, pp. 292-295,
Dec. 2008.
- [29] Tsai, P., Hu, Y.-C., and Yeh, H.-L.,
“Reversible Image Hiding Scheme Using
Predictive Coding and Histogram Shifting,”
Signal Processing, Vol. 89, No. 6, Jun.
2009.