

植基直方圖修改和差值擴張之無失真資訊隱藏技術

曾顯文

朝陽科技大學資訊管理系助理
教授

e-mail: hwtseng@cyut.edu.tw

吳啟璋

朝陽科技大學資訊管理所碩士
生

e-mail: s9514628@cyut.edu.tw

摘要

在這篇論文中，我們提出一個具可逆性的灰階影像資訊隱藏方法，當隱藏的資訊被取出的同時，影像也可以回復到最初的樣子。這個方法是基於直方圖的修改來達到可逆的目的，為了提高資訊的藏入量，我們以兩個鄰近像素間的差值來統計直方圖，以創造最大的藏入空間。透過實驗結果，我們可以發現到本篇所提出的方法可以有極高的影像品質及不錯的資訊藏入量。

關鍵詞：無失真資訊隱藏；直方圖修改；隱藏學；差值擴張。

1. 前言

網際網路是現今傳送資訊所使用的重要途徑，不限定使用者所在的地點和時間，無論何時都可以輕鬆簡單獲得想要的資訊，但是若只是單純傳送資訊而不對資訊加以保護及加密的話，則很容易被不懷好意的使用者所盜用。現今有許多技術可以對資訊進行保護的動作，這樣做雖然是提高了安全的層級，但反而會讓惡意的使用者明確知道有秘密資訊的存在，因此，一種名為「data hiding」又稱「Steganography」的技術被發明出來了，並廣泛地被應用在各種領域上。何謂「資訊隱藏」呢？顧名思義，就是把秘密資訊藏在某種媒介上，媒介的種類有：影像、影片、聲音、文字……等等，透過隱藏方法的處理後，媒介會產生變化，但所產生的變化是微小且人眼無法辨別的，透過這樣的處理後即可降低惡意的使用者的疑心，以便讓秘密資訊可以安全的傳送到合法接收方手上。雖然這樣的方式可以達到良好的安全性提升，但在某些方面的應用，如：軍事、醫學等，它可能需要的不只是取出秘密資訊而已，還要把媒介回復到原先的狀態，而這方面的研究也在近幾年被廣泛地討論及研究[1]-[9]。

而具有可逆性的資訊隱藏方法在最近比較具有代表性的有：Tian[1]在 2003 年提出的方法是以兩個鄰近的像素為一組，再加以擴張像素值間的差距來達到藏入的效果。基本上如果以擴張一次為原則且假設所有像素的配對皆有藏入資訊的話，它的資訊負載量是 0.5bpp，但為了還原原始的影像則必須記錄下一些額外的資訊，因此它的實際上的資訊負載量是小於 0.5bpp，如果為了藏入的需求而需要較大的資訊負載量的話，可以對影像進行多次的藏入動作以達到所需的要求，但相對地，影像的品質也會因此下降，這是無可避免的結果。而 Alattar[3]也在 2004 年的時候提出以向量為主來取代像素配對的隱藏方法，它是利用一個可逆式的整數轉換公式來轉換向量，如果該向量是屬於可擴張的話，就把秘密資訊藏入其中，並記錄下來該向量是否是屬於可擴張的，以便於取出秘密資訊及還原影像。而 Chang 等人[7]在 2006 年也提出了以鄰近像素間的差值來隱藏秘密資訊的方法。雖然 Alattar 的方法和 Chang 等人的方法都讓秘密資訊的藏入量大大地提高，但缺點就是它們仍然要記錄下大量的額外資訊。Ni 等人[9]在 2006 年所提出以直方圖修改的方式隱藏秘密資訊，根據實驗結果可以得知，該方法的藏入量是很少的，原因就在於一般影像的像素值集中在某一個點的機率是很小的，因而導致藏入量通常不大。

這篇論文的内容大綱如下：首先我們會簡短地說明 Ni 等學者[9]的方法，接著詳細地說明我們所提出的藏入和取出策略，然後「實驗結果」會呈現本篇方法的成果和分析，最後一個章節則總結本篇論文。

2. 相關文獻探討

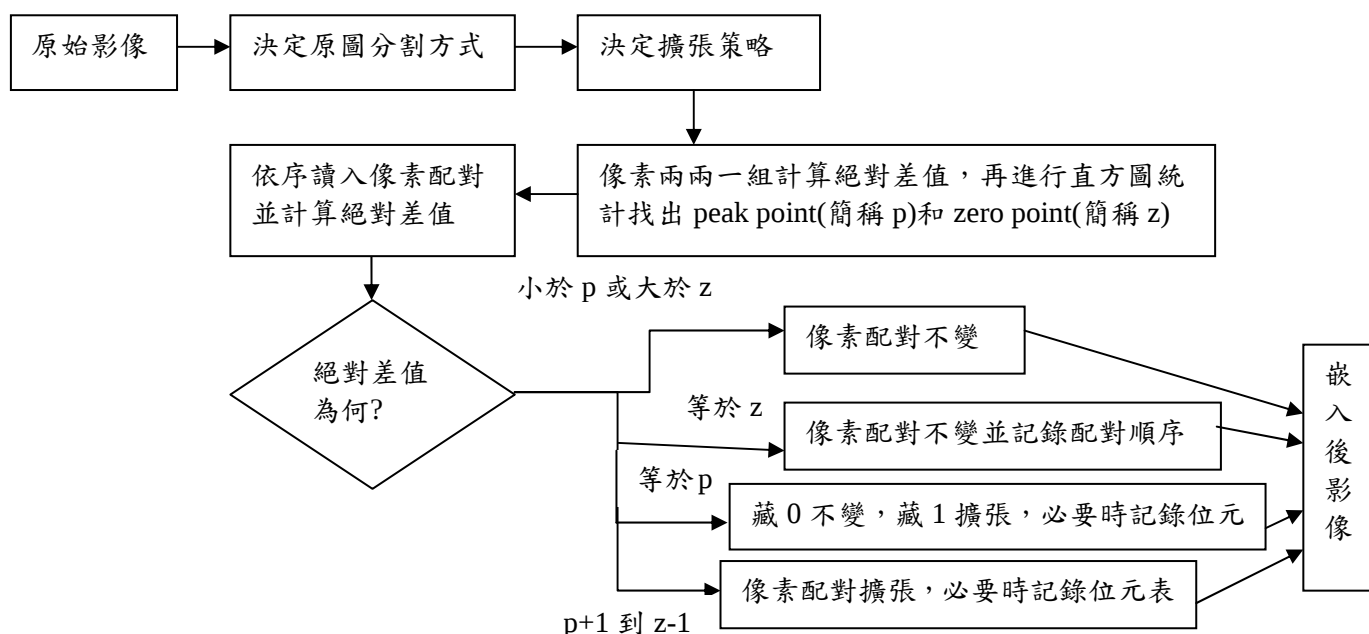
Ni 等學者[9]在 2006 年的時候提出了一個基於直方圖修改的資訊隱藏方法，以灰階影像來說，它統計了整張影像的像素值的數量，範圍為 0 到 255，再從其中挑選出一個統計量最高的像素值當作標的，稱為「peak point」，簡

稱為 p ，以此像素值為中心，在直方圖中向右或左找尋統計量為 0 的像素值當作「zero point」，簡稱為 z ，在此先以向右找尋為例，找到這兩個點以後，再決定原圖的像素點的掃描順序。再來就根據掃描順序一個接一個讀進像素，然後判斷它的值如果是介於 $p+1$ 到 $z-1$ 的話，就自動將此像素的值加 1；如果此像素的值是大於 z 或小於 p 的話就保持不變；如果此像素值為 p 時就可進行藏入秘密資訊的動作，我們先預先定義如果藏"0"的話就保持像素值不變，如果藏"1"的話就加 1，讓它的值變成 $p+1$ ，依照上面的原則，就可以對每個像素做最適合的處理。而如果在搜尋過程當中找不到統計量為 0 的像素值的話，則會找尋一個統計量最小的像素值，稱為「minimum point」來當作 z ，而在藏入過程中，如果讀入的像素的值為 z 的話，就要將它的座標位置額外記錄起來，使之可以無失真地還原成原始影像。為了提高藏入量，可以使用多組 p 和 z 的配對來進行藏入，但相對地影像品質(PSNR)就會比較低。以使用一組 p 和 z 來說， p 的統計量就是可以藏入的秘密資訊數量，一般來說它的可藏入數量是有限的，因為像素值的集中性不高，但相對地 PSNR 最起碼有 48dB 以上。

而在取出秘密資訊並還原回原圖時，我們必須知道的資訊為 p 、 z 、影像像素的掃描順序以及被記錄的座標位置，根據掃描順序我們一個接一個讀進像素，如果它的值是大於 z 或小於 p 的話就保持不變，如果它的值是介於 $p+2$ 到 z 且不為被記錄下的座標位置的話，就把它做減 1 的動作，若值為 z 且是被記錄下的位置的話就保持不變，若值為 p 則取出秘密資訊"0"並保持不變，若值為 $p+1$ 則取出秘密資訊"1"並把它做減 1，根據上面的方式就可以把藏入的秘密資訊全部取出來並把被修改過後的影像回復到原來的樣子。

3. 研究方法

由於 Ni 等學者[9]提出的方法有藏入量太少的缺點，在實際應用上可能無法滿足需求，因此本篇論文提出了改良的版本，我們利用相鄰像素做配對，再計算其絕對差值進行統計，由於相鄰像素具有相似的特性，因此其差異值會有集中的效果，進而獲取大量的 peak point 統計量，提高影像的藏入量，詳細的藏入過程如下：



圖(a) 研究方法藏入流程圖

3.1 藏入演算法

(一) 先決定原圖切割方式，以 512×512 大小的灰階影像為例，我們可以決定完全不切割，以 512×512 來進行藏入動作或者把原圖切割成四大塊，每塊大小為 256×256 ，再分別來進行藏入動作，當然也可以往下再進行切割，依此類推。當切割的越小時所要記錄的 peak point 和 zero point 就越多，也會連帶降低實際藏入量。

(二) 將原圖的全部像素以兩個像素為一組配對，再依像素配對的順序來掃描做判斷，如果像素配對內的兩個像素的值若任何一個為 0 或 1 時，則將 Min 做加 1 的動作，Min 是用來儲存原圖中像素配對的任一像素的值為 0 或 1 的像素配對個數；而如果像素配對內的兩個像素的值若任何一個為 254 或 255 時，則將 Max 做加 1 的動作，Max 是用儲存原圖中像素配對的任一像素的值為 254 或 255 的像素配對個數。依序掃描完畢後，再根據 Min 和 Max 的大小決定在進行像素配對擴張時所要採取的策略，如果 Min 大於等於 Max 時，就決定全圖的像素配對如果在需要擴張時都採取往像素值較大者擴張的修改方式，反之，如果 Max 大於 Min 時，則決定全圖的像素配對如果在需要擴張時採取往像素值較小者擴張修改的方式，如果兩個像素值相同且需要進行擴張的話，預設是配對左邊第一個的像素進行擴張修改的動作。這個步驟的目的主要是降低位元表的記錄數量。

(三) 進行完上面的動作後，我們以兩個像素為一組當作配對，之後把全部像素配對的絕對差值求出，再把每個像素配對的絕對差值集合起來進行直方圖的統計，再到直方圖內找尋統計量最大的絕對差值為何，因為像素配對是以像素和它鄰近的像素進行配對，因此基本上差異程度絕大部分都不大，因此當我們到直方圖內找尋統計最大的絕對差值時，絕大多數的情況都會在絕對差值 0 到 5 之間找到，而其他狀況實屬少數。而以實驗來看，大多都是在絕對差值 1 的地方統計量最高。當找到該絕對差值後，我們把該絕對差值當作是 peak point，簡稱為 p，並向右找尋統計量為 0 的絕對差值來當作 zero point，簡稱為 z。一般來說以絕大多數的影像來看都可以找到，如果無法找到的話，就改找尋統計量最小的絕對差值當作 z，並將屬於該絕對差值的像素配對的順序記錄

起來，以 512×512 的灰階圖來說就有 512×256 個配對，因此要記錄下一個配對需要花費 17 個位元來記錄。

(四) 選定好 p 和 z 了以後，依照自定的掃描順序進行藏入，掃描順序必須要記錄下來，當讀入每一組像素配對後，我們計算它的絕對差值，如果它的絕對差值小於 p 或大於 z 的話則此像素配對保持不變；如果絕對差值的範圍為 p+1 到 z-1 的話，則根據步驟(二)的結果決定如何擴張，有兩種策略，以往像素值較大者擴張的修改方式為例：

判斷此配對哪個像素較大，假設左邊像素較大，就將左邊像素的值加 1，這樣就完成了擴張的動作了，但如果原來的左邊像素的值為 254 時，當進行完擴張變成 255 後，我們必須在位元表記錄額外資訊，而如果原來的左邊像素的值為 255 時，我們無法使用往像素值較大者擴張的策略，因為會產生溢位的情況發生，因此該像素配對改採用往像素值較小者擴張的策略，把像素配對當中像素值較小者做減 1 的動作來擴張配對的差值同樣的也在位元表記錄額外資訊。如果絕對差值為 z 時則該像素配對保持不變，這種情況只有在找不到統計量為 0 的 z 時才會發生，另外把像素配對的順序記錄到順序表內。當絕對差值為 p 時，當我們要藏入的位元為 "0" 時，該像素配對保持不變，而藏入的位元為 "1" 時，就進行擴張的動作，也就是如同上面一樣的擴張方式。而如果在步驟(二)時決定以往像素值較小者擴張的策略，則在擴張時是把配對中像素值較小者減 1，如果原較小像素的值為 1 時，經減 1 成 0 後需在位元表記錄額外資訊，如果原較小像素的值為 0 時，因為溢位情況會產生，所以該配對改採像素值較大者加 1 的方式進行擴張並在位元表記錄下額外資訊。

依上面的步驟就可以把秘密資訊藏入到原圖內了，而如果當初是把原圖切割成多個區塊時，只要針對每個區塊進行上面的步驟即可，而每一個區塊必須要儲存一組的 p 和 z。而如果要進行多階段藏入時，建議採用和上一階段相反的擴張方式以避免影像品質下降太快。

3.2 取出演算法

而在取出秘密資訊和還原回原圖方面，必須知道影像的切割方式和原圖整體擴張的策略，像素的配對方式、每個區塊的 p 和 z 以及

避免還原時會造成誤判的位元表和原先絕對差值就落在 z 的像素配對的順序表、原圖的像素配對群的掃描順序也是必須要知道的。當進行還原動作時，如果像素配對的絕對差值小於 p 或大於 z 時就保持不變，而如果絕對差值為其他情形時有兩種還原的策略，以原圖全體採往像素配對較大者擴張策略的取出為例：

根據切割方式可以知道有幾個區塊，將像素配對一個接一個讀入，如果絕對差值為 z 時，如果它的像素配對的順序位於順序表內的話就保持不變且刪除所對應在順序表內的資料記錄，而如果不在順序表內的話就進行還原的動作，還原時把較大的像素做減 1 的動作除非較大像素的值為 255 時就要另外到位元表內取出最前面的位元來判斷把像素配對像素值較大者減 1 或將較小者加 1，如果還原時需要動到位元表來輔助時，在還原後就把位元表中的相對應的位元刪除。如果絕對差值為 p 時就取出藏入的位元 "0"，並且該像素配對保持不變。如果絕對差值為 $p+1$ 或絕對差值在 $p+2$ 到 $z-1$ 之間時將該像素配對進行還原的動作，還原時的處理和絕對差值為 z 且像素配對不在順序表內的處理一樣，如果絕對差值為 $p+1$ 則取出藏入的位元 "1"。而原圖全體採往像素配對較小者擴張策略的取出和上述像素配對較大者的取出方式的大致相同，只有還原時不同，還原時把把較小的像素做加 1 的動作除非較小像素的值為 0 時就要另外到位元表內取出最前面的位元，以便來判斷把像素配對像素值較大者減 1 或將較小者加 1，如果還原時需要動到位元表來輔助時，在還原後就把位元表中的相對應的位元刪除。

4. 實驗結果

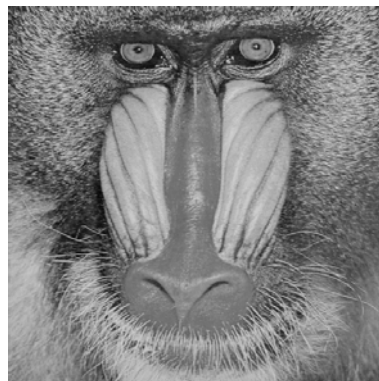
在這個章節中，我們將會呈現出所提出方法的實驗結果，而六張灰階影像：Lena、Airplane、Baboon、Pepper、Boat、Tiffany 是拿來實驗的原始影像，它們的長寬皆為 512×512 ，而我們拿來評估影像品質的指標為 PSNR(peak signal-to-noise ratio)，它的公式如下：

$$PSNR = 10 \log \frac{255^2}{MSE} dB$$

$$MSE = \left(\frac{1}{M \times N} \right) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (\alpha_{ij} - \beta_{ij})^2$$

其中 M 和 N 代表影像的長寬， α_{ij} 代表原始影像在座標 (i,j) 的像素值， β_{ij} 代表嵌入秘密資訊的影像在座標 (i,j) 的像素值，而較高的 PSNR 值代表原始影像和嵌入秘密資訊的影像之間的差異以人眼來看是很難分辨出的，一般來說，如果 PSNR 值大於 30dB 的話，以人眼來分辨大多分辨不太出來。

圖(b)、(c)、(d)、(e)、(f)、(g)分別是以本方法在完全不切割的影像進行藏入秘密資訊，可以看到它們幾乎和原圖無異，因為它們的 PSNR 值非常高，都有 51dB 以上的表現，平均為 51.69dB，而詳細的實驗結果可以在表(一)當中可以更清楚地觀察到，在藏入量方面是和實驗影像本身的像素值分佈有著密不可分的關係，舉例來說，Airplane 因為它影像本身大多屬於平滑區域，因此像素和像素之間的差距較小，因此它的藏入量也相對較大；而以 Baboon 來說，因為它影像絕大多數都屬於複雜區域，所以像素和像素之間的差距較大，相對來說藏入量就不大了。舉 Lena 來說，因為以不切割的方式藏入，所以只有一組 p 和 z 需記錄，花費 16 個位元，而記錄像素和像素如何配對以及影像採用哪種藏入策略各需花費 1 個位元，總計 2 個位元，而 Lena 的藏入過程中沒有順序表和位元表，實際藏入量為 $27514(\text{藏入量}) - 16 - 2 = 27496(\text{位元})$ ，如果實驗影像有順序表或位元表的記錄則在計算實際藏入量時需扣除掉其所佔空間。實驗影像的平均實際藏入量為 25255.5(位元)，而從 bpp(bits per pixel)來看，平均有 0.0964(位元)。圖(h)是 Lena 中的兩個像素為一組的像素配對的絕對差值統計直方圖，圖(i)為 Lena 像素的像素值的統計直方圖，圖(j)是 Baboon 中的兩個像素為一組的像素配對的絕對差值統計直方圖，圖(k)為 Baboon 像素的像素值的統計直方圖，由此我們可以從直方圖的差異可以看出本篇方法和 Ni 等學者提出方法之間的藏入量的多寡，也由此證明本篇方法較優於 Ni 等學者提出的方法。



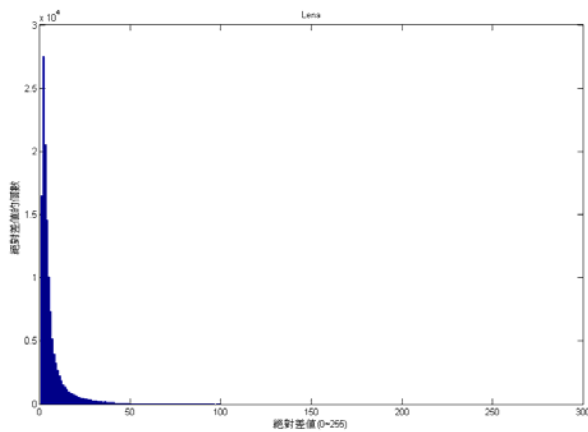
圖(b)Lena PSNR=51.73(dB) 圖(c)Airplane PSNR=51.98(dB)圖(d)Baboon PSNR=51.36(dB)



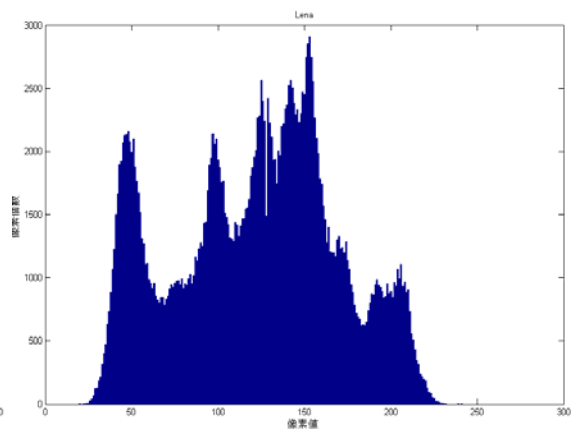
圖(e)Pepper PSNR=51.73(dB) 圖(f)Boat PSNR=51.58(dB) 圖(g)Tiffany PSNR=51.75(dB)

表(一)本研究方法的實驗結果

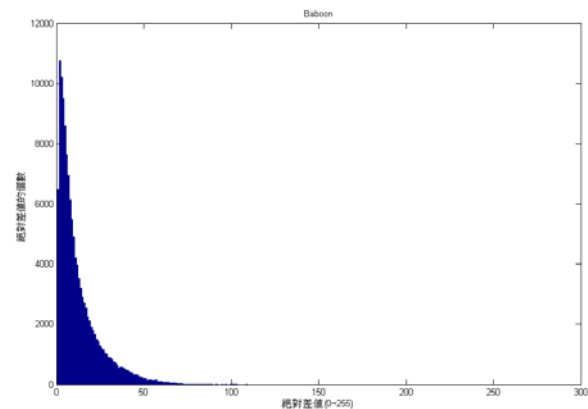
影像名稱	方法	PSNR(單位：dB)	實際藏入量(單位：位元)	bpp
Lena	Ni 等學者[9]	48.2	5460	0.0208
	本研究方法	51.73	27496	0.1049
Airplane	Ni 等學者[9]	48.3	16171	0.0617
	本研究方法	51.98	33593	0.1281
Baboon	Ni 等學者[9]	48.2	5421	0.0207
	本研究方法	51.36	10746	0.0410
Pepper	Ni 等學者[9]	48.2	5449	0.0208
	本研究方法	51.73	28696	0.1095
Boat	Ni 等學者[9]	48.2	7301	0.0279
	本研究方法	51.58	24056	0.0918
Tiffany	Ni 等學者[9]	48.2	8782	0.0335
	本研究方法	51.75	26946	0.1028
平均	Ni 等學者[9]	48.22	8097.3	0.0309
	本研究方法	51.69	25255.5	0.0964



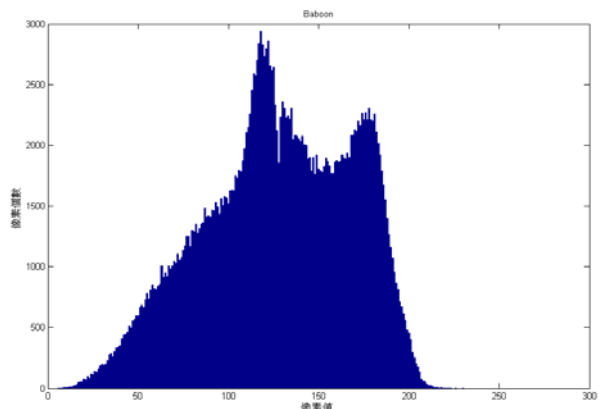
圖(h)Lena 像素配對絕對差值統計直方圖



圖(i)Lena 像素值統計直方圖



圖(j) Baboon 像素配對絕對差值統計直方圖



圖(k) Baboon 像素值統計直方圖

5. 結論

在這篇論文中，我們提出了一個基於直方圖修改和差異擴張的方法，這是一個高藏入量和低失真度的可逆性資訊隱藏方法，修改直方圖內的部分內容是為了創造一個統計量為 0 的額外空間以便用來進行藏入的處理，而 peak point 和 zero point、順序表及位元表的記錄則是為了還原成原始影像的必要需求。從實驗結果中可以清楚地看出，我們的方法比 Ni 等學者提出的方法有著更好的影像品質和更高的藏入量。

參考文獻

- [1] J. Tian(2003), "Reversible Data Embedding Using a Difference Expansion," *IEEE Trans. Circuits Syst. and Video Technol.*, Vol. 13, no. 8, pp. 890-896.
- [2] A. M. Alattar(2004), "Reversible Watermark Using Difference Expansion of Quads," *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Vol. 3, pp. 377-380
- [3] A. M. Alattar(2004), "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," *IEEE Trans. Image Processing*, Vol. 13, no. 8, pp. 1147-1156.
- [4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber(2005), "Lossless Generalized -LSB Data Embedding," *IEEE Trans. Image Processing*, Vol. 14, no. 2, pp. 253-265
- [5] C. C. Cheng, W. L. Tai, and M. H. Lin(2005), "A Reversible Data Hiding Scheme with Modified Side Match Vector Quantization," *Proc. Int. Conf. Advanced Information Networking and Application*, Vol. 1, pp. 947-952.
- [6] L. Kamstra and Henk J. A. M. Heijmans(2005), "Reversible Data Embedding Into Images Using Wavelet Techniques and Sorting," *IEEE Trans. Image Processing*, Vol. 14, no. 12, pp. 2082-2090
- [7] C.C. Chang, T.C. Lu, A difference expansion oriented data hiding scheme for restoring the

- original host images, *J. Syst. Software* Vol.79 No.12 (2006) 1754 – 1766
- [8] S. K. Yip, O. C. Au, H. M. Wong, and C. W. Ho(2006), “Generalized lossless data hiding by multiple predictors,” *International Symposium on Circuits and Systems (ISCAS) 2006*, pp. 21-24
- [9] Z. Ni, Y. Q. Shi, N. Ansari and W.Su(2006), “Reversible Data Hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, Vol. 16, no. 3, pp. 354-362