

多層式可逆資訊隱藏技術應用邊緣敏感度分析方法

呂慈純 黃英軒 許永明

朝陽科技大學 資訊管理系

tclu@cyut.edu.tw

摘要

本文提出一個可逆式資訊隱藏技術，該技術先利用 Lukac 預測法以產生預測值，再透過所提出的藏入規則將機密資訊嵌入於預測誤差值中。由於該規則僅針對預測誤差值進行加減 1 之修改，故偽裝像素與原始像素之間差異是相當小的。因此，若重複藏入機密資訊時，使用這些偽裝像素所產生的預測值與使用原始像素所產生的預測值會非常相似，故可允許嵌入更多機密資訊，並且維持良好的影像品質，實驗結果顯示所提方法可達到高藏入率與保持高影像品質。

關鍵詞：可逆式資訊隱藏技術、Lukac 預測法、影像品質。

Abstract

This paper proposes a reversible data hiding technique that uses Lukac prediction method to produce a prediction value and then embeds the secret data into the prediction error by using the proposed embedding rules. Since we modify the prediction error by only increasing or decreasing one, the difference between the stego pixel and original pixel is small. Thus, for the iterative embedding, the prediction value generated by the stego pixel is very similar to that generated by the cover pixel. As a result, the pixel is allowed for embedding more secret data and remaining good image quality. Experimental results display that the proposed method can accomplish high hiding rate and keep high image quality.

Keywords: reversible data hiding technique, Lukac prediction method, image quality.

1. 前言

隨著網際網路的蓬勃發展，利用網路來傳遞訊息的方式已逐漸地取代以往書信通訊。然而，在網路傳輸過程中，許多機密資訊須要保密，以避免不法第三者的竊取、竄改或破壞等攻擊，故學者們提出可逆式資訊隱藏技術，該技術將機密資訊嵌入於數位多媒體中(Multimedia)以欺瞞駭客；此外，藉由取出和還原演算法將機密資訊取出，並百分之百還原原始多媒體。

在 2003 年，Tian 學者提出差值擴張隱藏法(Difference Expansion) [1]，該方法計算兩個相鄰像

素的平均值和差值，再將差值擴張成二倍以嵌入一個機密位元。該方法無須複雜的計算，但擴張較大的差值會產生嚴重的影像失真和像素溢位問題(Underflow or Overflow Problem)。2006年，Ni等學者提出一個直方圖隱藏法[2]，該方法先統計掩蔽影像中各個像素值之出現次數，再製成一張直方圖。在直方圖中，最常出現的像素稱為峰值(Peak Point)，這些最常出現的像素可用來藏機密資訊。

2010年，Lee等學者提出一個基於預測方法的可逆式資訊隱藏技術[3]，該技術計算兩個相鄰像素(即上方像素和左方像素)的平均值作為預測值，接著，計算原始像素與預測值之間的差值，若預測誤差值小於事先定義的門檻值，則利用差值擴張方法[1]將機密資訊藏入於像素中；否則，利用直方圖位移技術[2]修改像素。該藏入規則顯示若預測差值愈小或門檻值愈大，則藏入效能愈好。雖然調高門檻值可允許更多像素嵌入機密資訊，然而，擴張預測誤差後，影像會產生嚴重的失真問題。

為了降低像素與預測值之間的誤差，Lee和Chen學者[4]於2012年使用像素的四個相鄰像素(即上、下、左和右像素)的平均值作為預測值，再利用Lee等學者提出的藏入規則[3]進行資訊隱藏。由於四個相鄰像素的平均值比二個相鄰像素的平均值有更準確的預測率，故此方法的藏入量和影像品質比Lee等學者的方法好。然而，該方法為了藏入大量的機密資訊，必須調高門檻值，導致擴張較大的預測誤差和大幅修改像素值。由於像素有嚴重的失真問題和它將是下一個掩蔽像素的預測值，故像素的預測準確率會大幅降低，從而同時降低藏入效能和影像品質。

為了克服此缺失，本文提出一個低失真像素修改法。在藏入機密資訊過程前，先利用 Lukac 預測法計算相鄰像素之間的敏感係數，換言之，所提方法計算相鄰像素之間的關係，進而推導出更好的預測值。接下來，所提方法將像素進行加減 1 之修改，以嵌入機密資訊。由於像素僅做加減 1 之修改，故像素的預測準確率不會下降太多，因此，所提方法可嵌入大量機密資訊和僅產生輕微的影像失真。

2. 文獻探討

2.1 Lukac 演算法

Lukac 等學者於 2004 年提出一個預測法[5]，該方法可有效解決彩色像素遺失之問題。Lukac 預測

法如下所示：

步驟 1: 針對欲預測的像素值 $P_{(i,j)}$ ，計算其四個鄰近像素 NP_t ($t = 1, 2, \dots, 4$) 的邊緣敏感係數 ES_t ，其中四個鄰近像素 NP_t 是像素 $P_{(i,j)}$ 的上下左右四個鄰近像素。邊緣敏感係數的公式如下所示：

$$ES_t = \frac{1}{1 + \sum_{l=1}^4 |NP_l - NP_t|} \quad (1)$$

步驟 2: 將每一個邊緣敏感係數 ES_t 進行正規化，以得到鄰近像素 NP_t 的權重值 w_t ，其正規化公式為：

$$w_t = \frac{ES_t}{\sum_{l=1}^4 ES_l} \quad (2)$$

步驟 3: 將步驟 2 所得到的權重值 w_t 與鄰近像素 NP_t 進行相乘，再將四個相乘結果進行加總，便可得到預測值 $\hat{P}_{(i,j)}$ ，如：

$$\hat{P}_{(i,j)} = \left[\sum_{t=1}^4 NP_t \times w_t \right] \quad (3)$$

上述步驟顯示了若相鄰像素與其它三個相鄰像素的差異較大時，則該相鄰像素可能是一個邊緣像素或是雜訊值，因此，其邊緣敏感係數和權重值較低，以避免該邊緣像素或雜訊值降低預測準確率；相反地，若相鄰像素與其它相鄰像素之間的差異較小時，則表示相鄰像素之間具有高度的關聯性，其可增加預測準確率，因此，邊緣敏感係數和權重值較高，進而產生一個精確的預測值。

2.2 可調整預測的無失真資訊隱藏技術

Lee 和 Chen 學者於 2012 年提出一個可調整預測的無失真資訊隱藏技術[4]，該技術計算目前像素 $P_{(i,j)}$ 的鄰近像素平均值作為一個預測值 $\hat{P}_{(i,j)}$ ，如：

$$\hat{P}_{(i,j)} = \begin{cases} \left[\frac{\hat{P}_{UL} + \hat{P}_{UR} + \hat{P}_{DL} + \hat{P}_{DR}}{4} \right], & \text{if } 2 \leq i \leq H-1 \text{ and } 2 \leq j \leq W-1 \\ \left[\frac{\hat{P}_{UL} + \hat{P}_{UR}}{2} \right], & \text{if } i = H \text{ and } 2 \leq j \leq W-1 \\ \left[\frac{\hat{P}_{UL} + \hat{P}_{DR}}{2} \right], & \text{if } 2 \leq i \leq H-1 \text{ and } j = W \\ \hat{P}_{UL}, & \text{if } i = H \text{ and } j = W \end{cases} \quad (4)$$

其中， (i,j) 表示像素的座標； H 和 W 表示影像之長與寬； \hat{P}_{UL} 表示上方像素 $P_{(i-1,j)}$ 與左方像素 $P_{(i,j-1)}$ 的整數平均值； \hat{P}_{UR} 表示上方像素 $P_{(i-1,j)}$ 與右方像素 $P_{(i,j+1)}$ 的整數平均值； \hat{P}_{DL} 表示下方像素 $P_{(i+1,j)}$ 與左方像素 $P_{(i,j-1)}$ 的整數平均值； \hat{P}_{DR} 表示下方像素 $P_{(i+1,j)}$ 與右方像素 $P_{(i,j+1)}$ 的整數平均值，公式如下所示：

$$\hat{P}_{UL} = \left[\frac{P_{(i-1,j)} + P_{(i,j-1)}}{2} \right], \quad (5)$$

$$\hat{P}_{UR} = \left[\frac{P_{(i-1,j)} + P_{(i,j+1)}}{2} \right], \quad (6)$$

$$\hat{P}_{DL} = \left[\frac{P_{(i+1,j)} + P_{(i,j-1)}}{2} \right], \quad (7)$$

$$\hat{P}_{DR} = \left[\frac{P_{(i+1,j)} + P_{(i,j+1)}}{2} \right]. \quad (8)$$

當我們得到預測值 $\hat{P}_{(i,j)}$ 後，便可計算掩蔽像素 $P_{(i,j)}$ 與預測值 $\hat{P}_{(i,j)}$ 之間的絕對差值 $e_{(i,j)}$ ，其公式為 $e_{(i,j)} = |P_{(i,j)} - \hat{P}_{(i,j)}|$ 。若絕對差值 $e_{(i,j)}$ 等於或小於門檻值 T ，則像素 $P_{(i,j)}$ 使用公式(9)藏入一個機密訊息 s 。

$$P'_{(i,j)} = \begin{cases} \hat{P}_{(i,j)} + 2 \times e_{(i,j)} + s, & \text{if } P_{(i,j)} \geq \hat{P}_{(i,j)} \\ \hat{P}_{(i,j)} - 2 \times e_{(i,j)} - s, & \text{otherwise} \end{cases} \quad (9)$$

其中，機密訊息 s 值為 0 或 1。否則，若絕對差值 $e_{(i,j)}$ 大於門檻值 T ，則使用公式(10)修改像素 $P_{(i,j)}$ ，進而得到偽裝像素 $P'_{(i,j)}$ 。

$$P'_{(i,j)} = \begin{cases} P_{(i,j)} + T + 1, & \text{if } P_{(i,j)} \geq \hat{P}_{(i,j)} \\ P_{(i,j)} - T - 1, & \text{otherwise} \end{cases} \quad (10)$$

3. 所提方法

在所提方法中，每個掩蔽像素可藉由 Lukac 預測法產生預測值，再利用所提出的嵌入規則將機密資訊藏入於預測誤差中，並將此帶有機密資訊的誤差值加入於掩蔽像素中，以產生偽裝像素。詳細的藏入演算法如下所示：

步驟 1: 使用者設定門檻值 T 。

步驟 2: 每個掩蔽像素 $P_{(i,j)}$ 可分成參考像素或可嵌入像素，其分類公式為 $c = (i+j) \bmod 2$ ，其中， i 和 j 表示像素在影像中的座標。若 c 為 0，則表示此像素是可嵌入像素；否則，若 c 為 1，則該像素為參考像素。這些可嵌入像素藉由以下步驟來隱藏資訊。

步驟 3: 建立一個嵌入常數值 n ，令 $n = 1$ ，表示嵌入第一回合。

步驟 4: 對每個可嵌入像素使用 Lukac 預測法，以產生一個預測值 $\hat{P}_{(i,j)}$ ，其中 Lukac 預測法請參閱本文的子章節 2.1。

步驟 5: 計算掩蔽像素 $P_{(i,j)}$ 和預測值 $\hat{P}_{(i,j)}$ 之間的誤差 $e_{(i,j)}$ ， $e_{(i,j)} = P_{(i,j)} - \hat{P}_{(i,j)}$ 。

步驟 6: 若預測誤差 $e_{(i,j)}$ 等於門檻值 T 或 $(-T + 1)$ ，則可藏一個機密資訊 s 至掩蔽像素 $P_{(i,j)}$ 中，其藏入公式如下：

$$P'_{(i,j)} = \begin{cases} P_{(i,j)} + s, & \text{if } e_{(i,j)} = T \\ P_{(i,j)} - s, & \text{if } e_{(i,j)} = -T + 1 \end{cases} \quad (11)$$

否則，若預測誤差 $e_{(i,j)}$ 大於門檻值 T 或它小於 $(-T + 1)$ ，則不允許嵌入任何機密訊息至

像素 $P_{(i,j)}$ 中，並使用公式(12)修改像素 $P_{(i,j)}$ ，以得到偽裝像素 $P'_{(i,j)}$ 。

$$P'_{(i,j)} = \begin{cases} P_{(i,j)} + 1, & \text{if } e_{(i,j)} > T \\ P_{(i,j)} - 1, & \text{if } e_{(i,j)} < -T + 1 \end{cases} \quad (12)$$

步驟 7: $n = n + 1$ ，並將步驟 6 所得到的偽裝像素當作參考像素，未被修改之參考像素視為掩蔽像素，其像素分類公式為 $c = (i + j + 1) \bmod 2$ ，再將這些掩蔽像素代入步驟 4 到 7。當 $n = 2$ ，則表示所有像素皆已藏入。

步驟 8: $T = T - 1$ 。

步驟 9: 若 $T = 0$ ，則完成隱藏程序；否則，重複執行步驟 2 到 9，將偽裝影像視為原始影像再藏一次。

我們使用一個例子來闡述機密資訊藏入之程序，其中門檻值 T 設為 1 和嵌入常數值 n 為 1。首先，我們使用分類公式 $c = (i + j) \bmod 2$ 將圖 1(a) 中的掩蔽像素分成可嵌入像素 ($c = 0$) 與參考像素 ($c = 1$)，其分類結果如圖 1(b) 所示。接著，座標 (2, 2)、(2, 4) 及 (3, 3) 的掩蔽像素皆具有四個鄰近像素值 (即上、下、左和右相鄰像素)，故可利用 Lukac 演算法得到預測值，如表 1(a) 所示。當我們得到預測值後，便可計算像素與預測值之間的誤差。

掩蔽像素 $P_{(2,2)}$ 的預測誤差值 $e_{(2,2)}$ 等於門檻值 T ，故可用來嵌入一個機密資訊。由於欲藏入的機密資訊 s 為 0，故無須修改像素值。掩蔽像素 $P_{(2,4)}$ 的預測誤差值 $e_{(2,4)}$ 等於門檻值 T ，因此，將機密資訊“1”加入於掩蔽像素 $P_{(2,4)} = 94$ 中，得到偽裝像素值 $P'_{(2,4)} = 95$ 。掩蔽像素 $P_{(3,3)}$ 的預測誤差值 $e_{(3,3)}$ 為 6，其值大於門檻值 T ，故無法嵌入機密資訊，此外，將此像素 $P_{(3,3)} = 90$ 進行加 1 之修改，修改結果如表 1(a) 所示。藏完機密資訊後的偽裝影像如圖 1(c) 所示。

為了嵌入更多的機密資訊，將嵌入常數值 n 加 1，並開始進行第二回合的嵌入程序。首先，使用分類公式 $c = (i + j + 1) \bmod 2$ 將圖 1(c) 中的像素分成可嵌入像素 ($c = 0$) 與參考像素 ($c = 1$)，其結果如圖 1(d) 所示。座標 (2, 3)、(3, 2) 及 (3, 4) 的像素值可利用 Lukac 預測法產生預測值，並進一步計算其預測誤差，如表 1(b) 所示。由於像素 $P_{(2,3)}$ 的預測誤差值 $e_{(2,3)}$ 等於 $(-T + 1)$ ，因此，嵌入一個機密資訊 $s = 1$ 於掩蔽像素 $P_{(2,3)} = 97$ ，得到偽裝像素 $P'_{(2,3)} = 97 - 1 = 96$ 。其餘二個預測誤差值 (即 $e_{(3,2)}$ 和 $e_{(3,4)}$) 小於 $(-T + 1)$ ，故無法嵌入機密資訊，此外，將這 2 個預測誤差值所對應的像素 ($P_{(3,2)}$ 和 $P_{(3,4)}$) 進行減 1 之修改，以得到偽裝像素，如表 1(b)。嵌入所有機密資訊後的偽裝影像如圖 1(e) 所示。

110	110	100	95	95
105	101	97	94	95
100	90	90	80	80
90	70	70	70	70

(a) 掩蔽影像

0	1	0	1	0
1	0	1	0	1
0	1	0	1	0
1	0	1	0	1

(b) 使用公式 $c = (i + j) \bmod 2$ 將像素分成可嵌入像素與參考像素之結果

110	110	100	95	95
105	101	97	95	95
100	90	91	80	80
90	70	70	70	70

(c) 第一回合藏入後的偽裝影像

1	0	1	0	1
0	1	0	1	0
1	0	1	0	1
0	1	0	1	0

(d) 使用公式 $c = (i + j + 1) \bmod 2$ 將第一回合所得到的像素分成可嵌入像素與參考像素之結果

110	110	100	95	95
105	101	96	95	95
100	89	91	79	80
90	70	70	70	70

(e) 嵌入所有機密資訊後的偽裝影像

圖 1 藏入機密資訊之範例

表 1 藏入範例的像素修改細節

(a) 第一回合

座標	原始像素	預測值	機密資訊	偽裝像素
(2, 2)	101	100	0	101
(2, 4)	94	93	1	95
(3, 3)	90	84	-	91

(b) 第二回合

座標	原始像素	預測值	機密資訊	偽裝像素
(2, 3)	97	97	1	96
(3, 2)	90	93	-	89
(3, 4)	80	84	-	79

當我們收到偽裝影像和門檻值 T 時，可藉由下列的取出和還原步驟來擷取機密資訊和還原掩蔽影像。

步驟 1: 建立一個取出和還原順序的常數值 n ，令 $n = 1$ 。

步驟 2: 將偽裝像素 $P'_{(i,j)}$ 分為帶有機密資訊的像素和參考像素，其分類公式為 $c = (i + j + 1) \bmod 2$ 。若 c 為 1，則表示該像素為參考像素；否則，若 c 為 0，則該像素可能帶有機密資訊，這些帶有機密資訊的像素 $P'_{(i,j)}$ 將被代入下列步驟，以取出機密資訊 s 和還原掩蔽像素 $P_{(i,j)}$ 。

步驟 3: 使用 Lukac 預測法，以產生每個偽裝像素

$P'_{(i,j)}$ 的預測值 $\hat{P}_{(i,j)}$ 。

步驟 4: 計算偽裝像素 $P'_{(i,j)}$ 和預測值 $\hat{P}_{(i,j)}$ 之間的差值 $e'_{(i,j)}$ 。

步驟 5: 使用公式(13)和(14)，以取出機密資訊 s 和還原掩蔽像素 $P_{(i,j)}$ 。

$$s = \begin{cases} 0, & \text{if } e'_{(i,j)} = k \text{ or } -k + 1 \\ 1, & \text{if } e'_{(i,j)} = k + 1 \text{ or } -k \end{cases}, \quad (13)$$

$$P_{(i,j)} = \begin{cases} P'_{(i,j)} - 1, & \text{if } e'_{(i,j)} \geq k + 1 \\ P'_{(i,j)} + 1, & \text{if } e'_{(i,j)} \leq -k \end{cases}, \quad (14)$$

其中, k 的初始值為 1。

步驟 6: 令 $n = n + 1$, 並將步驟 5 所還原的像素 $P_{(i,j)}$ 當作參考像素, 而步驟 5 的參考像素將視為帶有機密資訊的偽裝像素, 再代入步驟 2 到 6, 以取出機密資訊和還原像素。當 $n = 2$, 表示完成整張影像的取出。

步驟 7: 若 k 值等於門檻值 T , 則已取出所有機密資訊和還原掩蔽影像; 否則, 若 k 值小於門檻值 T , 則 k 值加 1, 並重複執行步驟 1 到步驟 7。

4. 實驗結果

我們實作所提方法與近年來的可逆式資訊隱藏方法[3-4], 分別使用嵌入率(Embedding Rate, ER)和尖峰訊號雜訊比(Peak Signal-to-Noise Ratio, PSNR)以評估方法之優劣。藏入率和尖峰訊號雜訊比之公式分別如下所示:

$$\text{嵌入率} = \frac{\text{機密資訊的數量}}{\text{掩蔽像素的數量}} \text{ (bpp)}, \quad (15)$$

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \text{ (dB)}, \quad (16)$$

$$\text{MSE} = \frac{\sum_{i=1}^H \sum_{j=1}^W (P'_{(i,j)} - P_{(i,j)})^2}{H \times W}. \quad (17)$$

其中, MSE 為掩蔽影像與偽裝影像之均方差(Mean Squared Error); H 和 W 分別表示影像之長與寬; $P'_{(i,j)}$ 和 $P_{(i,j)}$ 分別為偽裝像素和掩蔽像素; (i, j) 表示像素的座標。

圖 2 顯示四張灰階測試影像, 其長和寬皆為 512。圖 3 顯示所提方法與比較方法[3-4]的實驗結果, 其證明了在相同嵌入率下, 所提方法的 PSNR 值高於其它二個方法。這是因為 Lee 等學者的方法[3]對每個掩蔽像素僅使用二個鄰近像素(即左方像素與上方像素)的平均值作為預測值, 故影像中複雜區域會產生不精確的預測值。這個不精確的預測值除了無法嵌入機密資訊, 還須要修改掩蔽像素。相反地, 所提方法使用 Lukac 預測法以計算鄰近像素之邊緣敏感係數和權重值, 進而推導出一個精確的預測值。由於像素與預測值之間的誤差相當小, 故像素可嵌入機密資訊和僅產生微小的失真。這些優

點證明所提方法較 Lee 等學者的方法好。

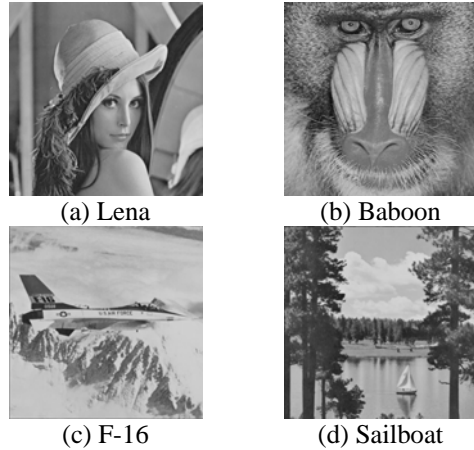
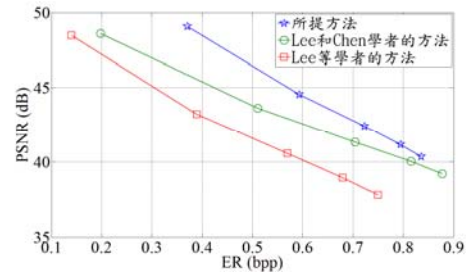
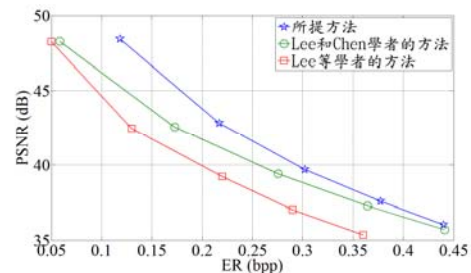


圖 2 四張測試圖像

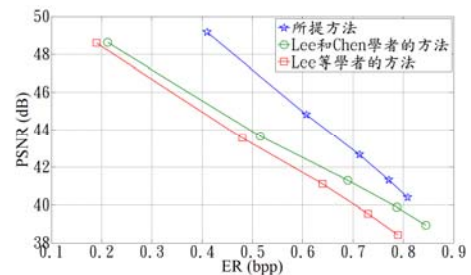
所提方法的偽裝影像品質高於 Lee 和 Chen 學者方法[4], 其原因是他們使用相鄰偽裝像素的平均值作為預測值, 而不是使用相鄰掩蔽像素的平均值, 故預測效能大幅降低, 進而導致藏入效能和偽裝影像品質下降。所提方法僅針對像素進行加減 1 之修改, 因此, 即使使用修改後的像素來產生預測值, 其預測結果仍然相當好, 故所提方法比 Lee 和 Chen 學者方法可嵌入更多的機密訊息和維持更好的影像品質。



(a) Lena



(b) Baboon



(c) F-16

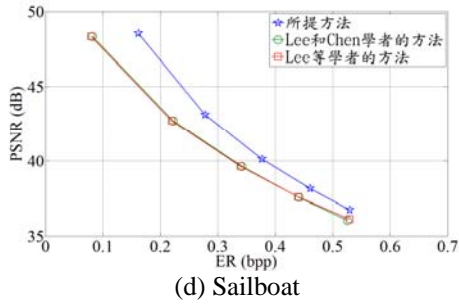


圖 3 所提方法與近年來的可逆式資訊隱藏方法之性能比較

5. 結論

所提方法首先使用 Lukac 預測法產生精確的預測值，由於像素與預測值的誤差相當小，故像素可允許嵌入機密資訊和僅產生輕微的影像失真。在嵌入機密資訊的過程中，我們僅對像素進行加減 1 的修改，故預測準確率不會大幅降低。這項優點證明了本文成功解決 Lee 和 Chen 學者方法的缺點。

參考文獻

- [1] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 890-896, 2003.
- [2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362, 2006.
- [3] C. F. Lee, H. L. Chen, and H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion," Journal of Systems and Software, vol. 83, no. 10, pp. 1864-1872, 2010.
- [4] C. F. Lee and H. L. Chen, "Adjustable prediction-based reversible data hiding," Digital Signal Processing, vol. 22, no. 6, pp. 941-953, 2012.
- [5] R. Lukac, K. Martin, and K. N. Platanoitis, "Digital camera zooming based on unified CFA image processing steps," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 15-24, 2004.